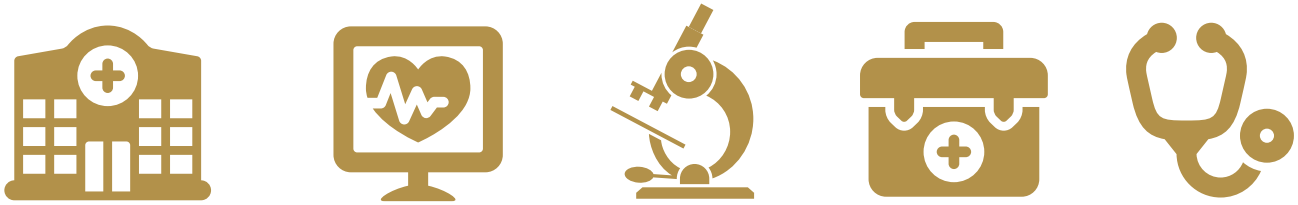
FOLEY

FOLEY & LARDNER LLP

Tapping Into the **Big Value** of Health Care **Big Data**

Top Legal and Regulatory Considerations on the Path to Monetization



Prepared by Foley's Health Care Industry Team and Privacy, Security & Information Management Practice

FOLEY

FOLEY & LARDNER LLP

Table of Contents

Executive Summary 1

Improving Care by Tapping Into the Data Goldmine 2

Big Opportunities Available in Big Data 4

Government Programs Supporting the Use of Big Data 6

Examining the Federal and State Legal Framework for Big Data 9

Key Federal Requirements for Big Data Types 12

Key State Laws Limiting the Use of Health Information 19

Despite Regulatory Challenges, Big Data Is Worth It 23

About the Authors 24

Appendix A — Overview of State Legal Framework

Appendix B — Select State Laws Governing Use and Disclosure of Health Data

FOLEY

FOLEY & LARDNER LLP

Executive Summary

Big Data — the ability to collect, process, and interpret massive amounts of information — has reached health care.

The proliferation of electronic medical records and mobile devices, enhanced computing platforms and infrastructure, new data sharing and mining tools, and other recent technological advances have dramatically increased the ability of health care providers, payors, and their affiliates to generate, aggregate, store, and analyze health information. Government agencies, health information exchanges, mobile device companies, online applications and platforms, social media, and collaborating hospitals, insurers, and physicians are accumulating vast amounts of health information. Rapid progress in data architecture, storage, and analysis has opened avenues to leverage that information in new and innovative ways.

Technology has created new business opportunities for health care entities — covered entities, business associates, and others — to use health data for financial purposes. This is true not only where the financial remuneration is for cash (e.g., the sale or marketing of a product using health data), but also in the creation of value for covered entities, their business associates, and third parties alike. Within health systems, Big Data will play a critical role in the move from volume-based care to value-based, accountable care. The ability to integrate, synthesize, and share complex health information can lead to enhanced coordination of care, potentially resulting in better health outcomes and lower costs.

Actualizing the promise of Big Data is not without its challenges — technical, institutional, operational, and legal. In many cases, the evolution of the law has not kept up with technology, resulting in a governing framework that is challenging to navigate. This paper will provide an overview of the U.S. federal and state considerations applicable to any business initiative that relies on Big Data, and provide some practical advice for those seeking to monetize Big Data in health care.

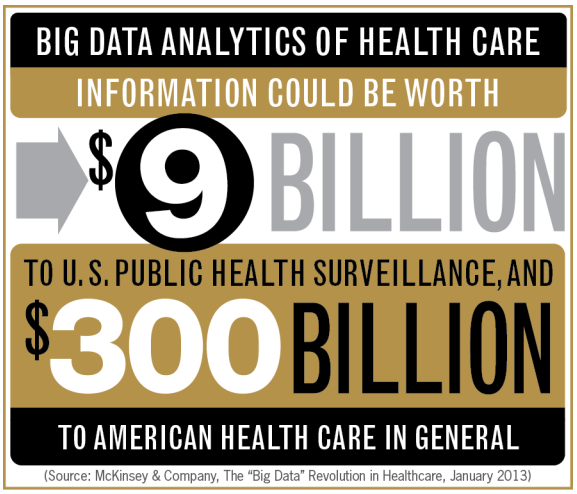
FOLEY

FOLEY & LARDNER LLP

Improving Care by Tapping Into the Data Goldmine

A recent article in *The New York Times Magazine* tells the story of a 13-year-old who presented at the hospital with symptoms of kidney failure. The physician team diagnosed lupus, but the combination of symptoms, including an inflamed pancreas and blood vessels along with kidney failure, triggered the concerns of the treating rheumatologist about the patient's potential for developing blood clots. The treating physicians saw no cause to give the patient anti-clotting drugs.

Upon reviewing scientific literature, the curious rheumatologist did not find any helpful studies. Undeterred, the rheumatologist searched a database of medical records of the hospital's lupus patients seen during the previous five years. The rheumatologist focused on lupus patients with similar symptoms, analyzing them to see if any patients developed blood clots. The database showed an increased risk of blood clots. Based on that information, the rheumatologist convinced the treating team to give the patient an anti-clotting drug.[1]



This real-life episode illustrates the potential value to be found in the increasingly vast troves of medical data. Organizing and accessing such data can improve health care outcomes. Additionally, secondary uses of these large datasets are creating unprecedented opportunities to derive value from health care data. McKinsey & Company estimates that Big Data analytics of health care information could be worth $9 billion to U.S. public health surveillance alone (by improving detection of and response to infectious disease outbreaks), and $300 billion to American health care in general.[2]

The opportunity to drive new business models is clear, but the challenges and obstacles inherent in leveraging that opportunity — technical, institutional, operational, legal, and so forth — are numerous and complex. The legal and regulatory landscape, which seeks to mitigate any potential misuse of confidential health information and protect legitimate privacy and security concerns, poses very real obstacles for organizations seeking to monetize health care data. Foley's Health Care and

FOLEY

FOLEY & LARDNER LLP

Privacy, Security & Information Management attorneys have developed this white paper to provide an overview of opportunities that are becoming increasingly available as a result of Big Data in health care, and the U.S. regulatory regime that is, in part, driving such industry change. We will then provide an overview of the key federal and state laws pertaining to the collection and secondary use of health data, and suggest strategies and best practices for addressing health privacy and data ownership concerns.

FOLEY & LARDNER LLP

Big Opportunities Available in Big Data

The aforementioned 13-year-old benefited from her medical team's ability to access a large volume of clinical data to arrive at a diagnosis. Big data also may be used in many ways, such as to contribute to advances in research, improvements in education, and in scientific discoveries.

A 2013 evaluation of the marketplace by McKinsey & Company revealed that more than 200 businesses created since 2010 are developing innovative tools to make use of available health care information.[3] The following is an overview of some of the areas in which health care data can be monetized.

» **Technology/Infrastructure — Data Storage, Security and Access.** Approximately 87 percent of U.S. hospitals currently have some form of electronic medical records, a percentage which is increasing rapidly.[4] The ability to store and share data in a secure and legally compliant environment is vital. Information technology companies are working to develop and implement solutions for better storage, security, and application of the data, and to create sets of tools to make better use of available health data.

» **Data Analytics.** Companies are sprouting up to develop data-driven solutions for supporting providers and population health management institutions. Organizations that can "connect the dots" to successfully organize and analyze data can expect to be rewarded.[5] In one recent example, Flatiron Health, a New York start-up that aims to detect useful patterns in medical records, recently raised $130 million from investors, including Google Ventures. Another Silicon Valley start-up, Enlitic, is using advances in machine learning to mine hospital data for otherwise invisible patterns and improve diagnoses.[6]

» **Expanding Data Access and Scaling Data Use.** Industry experts, researchers, employers, payers, and providers are using health care data to identify the most effective and cost-saving treatment protocols (e.g., comparative effectiveness research, patient monitoring), improve products and services (e.g., predictive modeling for new drugs, personalized medicine), and improve public health surveillance and response. While larger health systems may already have access to such troves of data by virtue of their size, *expanding* access to smaller providers, and *scaling* data use across organizations and populations faces multiple challenges, including respecting the privacy and security of personalized health information; balancing patient versus societal benefits; and considering stakeholder profits and political swings. In some cases, partnering can allow smaller systems to leverage the opportunities of data. Some large health systems, such as Duke

University, University of North Carolina, and University of Michigan, have worked to develop internal "centers of excellence" that leverage data to measure performance, identify best practices, and implement operational improvement projects.[7] This has created opportunities and access points for providers of secondary services and products designed to enable such scaling.

- **Marketing and Sales.** One of the most direct and effective methods for monetizing health information is using or sharing the information for marketing purposes. As discussed below, in certain cases, companies like Target have applied data analytics to target marketing initiatives without relying on protected health information to enter this tightly regulated field.

- **Research.** Using big data can help researchers mine an existing data set to test new hypotheses and provide the research community with new ways to capitalize on the wealth of data available. Recently, a National Institutes of Health (NIH)-funded researcher, Atul Butte, showed the benefits of utilizing big data to find new links between genes, diseases, and traits. Through the NIH's VARiants Informing MEDicine (VARIMED) database of more than 9,000 studies, his team found that 120 diseases and traits were linked to the interaction of only a handful of genes. While some of the disease-trait associations were previously known, new discoveries accounted for 20 percent of the findings. Following these findings, the NIH announced the launch of a new initiative called Big Data to Knowledge (BD2K), described below. Separately, in the summer of 2014, a consortium headed by Kaiser Permanente received a $7 million Patient-Centered Outcomes Research Institute (PCORI) grant to improve and advance the use of patient-centered outcomes research.

- **Web-Based Technologies.** The national trend toward increased population health management has resulted in a rise of mobile and web-based services that allow consumers to organize and store medical information from many sources, purchase health-related products through a website, or access or send information to a personal health record. Consumer-generated and controlled health data websites, such as PatientsLikeMe, include features that enable users to connect with others with similar health conditions; to track their personal health, fitness, caloric consumption and exercise; and to track medication use, including mobile device inhaler-use for asthmatics; and many others.

- **Mobile Applications.** There is also a rise of mobile and wearable devices and applications for gathering data and applying analytics. As of August 2014, at least 12 wearable device pilot projects were reportedly taking place at medical institutions across the country.[8] For example, Intel is partnering with the Michael J. Fox Foundation for Parkinson's Research in a new pilot aimed at using data mined from wearable devices to detect patterns in the progression of the disease.[9]

FOLEY

FOLEY & LARDNER LLP

Government Programs Supporting the Use of Big Data

The U.S. government has adopted initiatives and directives to encourage the government to make available government information and data to help meet identified objectives. These initiatives and directives, some of which are described below, reflect a clear governmental recognition of the value inherent in big data.

Open Government Initiative

On January 21, 2009, the first day of his presidency, President Obama issued two memoranda to executive branch agencies and departments designed to encourage transparency in government and to increase accessibility to government records. The first, "Transparency and Open Government," indicated the president's commitment to creating "an unprecedented level of openness in Government" and identified the goal of establishing a system of transparency, public participation, and collaboration. It charged the Office of Management and Budget (OMB) with developing an Open Government Directive that would direct executive departments and agencies to take action.[10]

In a second memorandum, President Obama addressed the administration of the Freedom of Information Act (FOIA). The memorandum reflected a commitment to accountability, stating that FOIA should "be administered with a clear presumption: In the face of doubt, openness prevails." He directed the attorney general to issue new, published guidelines governing FOIA to the heads of executive departments and agencies reaffirming the commitment to accountability and transparency.[11]

Several months later, on December 8, 2009, the director of the OMB issued an Open Government Directive (Directive) as directed by the president's "Transparency and Open Government" memorandum. It instructed executive departments and agencies to adopt and follow three core principles as the framework of an open government:

- **Transparency.** This promotes government accountability by providing the public with information about what the U.S. government is doing
- **Public Participation.** It allows members of the public to contribute ideas and expertise so that the government can make policies with the benefit of information that is widely dispersed in society
- **Collaboration.** This improves the effectiveness of government by encouraging partnerships and cooperation within the federal government, across levels of government, and between the U.S. government and private institutions

The Directive adopted these three principles and required executive departments and agencies to take a number of specified steps to implement them, including:

- **Publish Government Information Online.** Agencies were directed to place more information about their activities online, with a presumption of openness of their operations, though subject to legal limits for privacy, confidentiality, security, and other restrictions
- **Improve the Quality of Government Information.** Agency leaders were directed to make certain that

available information conforms to OMB guidelines on information quality, and to have systems in place to meet such requirement

- **Create and Institutionalize a Culture of Open Government.** Agency leaders were instructed to incorporate the values of transparency, public participation, and collaboration into the ongoing, day-to-day work of their agencies
- **Create an Enabling Policy Framework for Open Government.** Agencies were told that policies should evolve to realize the potential of technology in further enhancing open government

The OMB also directed each of the executive agencies to develop an Open Government Plan and to publish such a plan, reflecting the three core principles.

The two presidential memoranda and the Directive reflect a commitment from the top of our federal government for executive departments and agencies to make more information and data available to the general public. They reflect a recognition that the broader sharing of information will improve the functioning of government, will promote broader participation in government and policy, and, through collaborations, will open opportunities for scientific and other developments resulting from available data.

While the full effects of the Open Government Initiative will not be determinable for many years, the general assessment has been that the results are mixed. While certain agencies have been viewed as performing well in expanding access to information and meeting the principal action steps of the Directive, the performance of other agencies has not been as positive. In general, and perhaps not surprisingly, agencies focused on public security and law enforcement did not perform as well as other agencies in meeting both the terms of the Directive and their own aspirational goals that certain agencies initially set for themselves.[12] Despite the mixed results, the government policy still recognizes the value of sharing information and supports a presumption in favor of sharing more information and continuing in furtherance of the three core principles.

Big Data Research and Development Initiative

In March 2012, the U.S. Office of Science and Technology Policy (OSTP) announced a Big Data Research and Development Initiative (Initiative). Recognizing the potential value of big data, the Initiative was designed to "make the most of the fast-growing volume of digital data."[13] The Initiative seeks to improve the ability to extract knowledge and insights from the large and complex collection of digital data in the possession of the U.S. government. It also is consistent with the previously described Open Government Initiative.

In announcing the Initiative, the OSTP stated, "In the same way that past federal investments in information-technology R&D led to dramatic advances in supercomputing and the creation of the Internet, the initiative we are launching today promises to transform our ability to use big data for scientific discovery, environmental and biomedical research, education and national security."[14]

Accompanying the announcement of the Initiative, six federal departments and agencies made commitments of more than $200 million designed to:

- Advance core technologies to collect, store, preserve, manage, analyze, and share big data
- Harness the technology to increase discovery rates
- Expand the workforce using and developing these technologies

The National Science Foundation (NSF), one of six agencies that committed funds to support the Initiative, stated, "Data represents a transformative new currency for science, engineering and education."[15]

Use of big data to advance discoveries in health care and life sciences were a significant part of the initial agency commitments supporting the Initiative. The NSF and the National Institutes of Health (NIH) made a commitment to develop and improve techniques for utilizing data for imaging, molecular, cellular, electrophysiological, clinical, behavioral,

epidemiological, and clinical data sites in order to improve health care and for understanding and treating diseases. The NIH also announced that its data from the 1000 Genomes Project would be publicly available on the Amazon Web Services cloud, allowing researchers to have free access to the huge trove of data concerning human genetic variations.[16] To further support the Initiative, the NIH also announced the NIH BD2K program, with the goal of developing new approaches, standards, methods, tools, software, and competencies to capitalize on biomedical big data for research, implementation, and training.

Eighteen months after the initial announcement of the Initiative, additional projects supporting the Initiative were announced by federal agencies. The projects reflected significant collaborations between U.S. government agencies and leading private companies, universities, and other non-governmental organizations. At the time, it was suggested that 4.4 million jobs would be created by 2015 to support big data and the Initiative.

Health care-related collaborative projects that commenced in 2013 included:

- A collaboration among NIH, IBM, Geisinger Clinic, and Sutter Health to develop tools to identify patients at risk for heart failure
- A program with the American Society of Clinical Oncology to develop a computer network to unlock de-identified information from more than 170,000 patient care plans that otherwise would reside in private files, with the purpose of improving the quality of oncology care
- Development of a new platform through a Novartis, Pfizer, and Eli Lilly partnership to improve access to information gleaned from clinical trials[17]

The Initiative reflects a keen appreciation by the federal government and its agencies of the untapped potential and economic and scientific value of big data, both in leading to important discoveries and to creating economic growth. The initial focus of the Initiative is to develop technologies and methods to access and make use of big data, but it also reflects a commitment to make more government-controlled data available and to contribute federal resources, at times in collaborative approaches with non-governmental entities, to capitalize on the value offered by big data.

State Information Exchange Cooperative Agreement Program

Another program in which the federal government has promoted the sharing of data is the State Health Information Exchange Cooperative Agreement Program (Program). Enacted as part of The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), the Program made $564 million available to states and territories to encourage widespread use of electronic health records and health information exchanges. The Office of the National Coordinator for Health Information Technology (ONC) has established policies, standards, and services as part of the Program to promote the transporting of health information from point to point through secure, fast, and inexpensive channels.

The ONC made the funding available to states, or entities designated by a state's governor, to support the infrastructure for health information exchanges in states and territories. Of the $564 million, at least $4 million was made available to each state. The state designated entities (SDEs) overseeing the health information exchanges received the ONC funding, and set policies and frameworks for their own health information exchanges. The goal is to have functioning statewide systems capable of sharing health data, including lab reports and prescriptions, across unaffiliated organizations.

SDEs have taken various approaches as they develop health information exchanges. Factors such as the rural/urban mix of a state, the health care marketplace in a state, the state's history with health information exchanges, and local demand for services have affected both the pace and nature of the health information marketplace taken by various SDEs. The ONC grants have contributed to growth in health information exchanges.

FOLEY

FOLEY & LARDNER LLP

Examining the Federal and State Legal Framework for Big Data

There are no overarching privacy principles that uniformly apply to all patient health information. Federal and state laws co-exist with respect to the collection, use, and sharing of health information.

The determination of the legal requirements associated with monetization of health information — which depend on the type of data, the source of data, and the particular state with jurisdiction over such data — is a highly detailed and nuanced endeavor, but one with significant implications for structuring such initiatives.

As a threshold matter, any monetization initiative will need to consider the impact of the Health Insurance Portability and Accountability Act (HIPAA)[18] on the ability to achieve the goals of the initiative. HIPAA understandably can make it difficult for companies to obtain health information, and even more difficult to use that information for the purpose of data analysis, marketing, and other non-treatment purposes, without patient consent.

HIPAA applies to "protected health information," also commonly referred to as PHI, and includes demographic, clinical, payment, and financial information about an individual that is created or received by a "covered entity."[19] Thus, while the definition of PHI encompasses a broad range of information, generally speaking, HIPAA applies only to certain entities — health care providers, health insurance plans, and health care clearinghouses.

If your organization does not meet the definition of a covered entity, it may be a "business associate" with obligations to comply with the HIPAA Privacy and Security Rules. Generally speaking, a business associate is a service provider or other business partner to a covered entity that receives PHI from the covered entity. In addition to being covered under HIPAA, business associates will enter into a business associate agreement with the covered entity. The business associate agreement could require the business associate to comply with the provisions of HIPAA, in addition to other privacy and security requirements. Very often, these requirements will limit the business associate's ability to use and disclose PHI for any purpose other than in furtherance of the relationship between the covered entity and the business associate.

The business associate may be contractually prohibited from monetizing PHI by sharing it with third parties or other uses not directly related to the relationship between the covered entity and the business associate. Thus, where possible, the business associate should negotiate the ability to use PHI, or at least de-identified health information, received from the covered entity to further their monetization initiatives.

Depending on the context, not all health information may be covered under HIPAA. For example, HIPAA does not govern the health information in education records covered by the Family Educational Rights and Privacy Act (e.g., information generated in school health clinics), employment records held by a covered entity in its role as employer (e.g., records related to sick leave or records generated in an onsite health clinic), or information regarding a person who has been deceased for more than 50 years.

HIPAA also does not apply to the health information maintained in a personal health record (PHR) offered by an employer (separate from the employer's group health plan) or made available directly to an individual by a PHR vendor that is not a HIPAA covered entity. HIPAA also does not govern health information gathered directly from the consumer through online applications or mobile apps not provided by covered entities.[20] PHR providers not covered under HIPAA are governed by their own privacy policies and other applicable laws (e.g., state laws, the Federal Trade Commission (FTC) Act's prohibition against unfair and deceptive practices, and so forth). Often a patient will allow his or her health care provider to add health information to the PHR. In these instances, the information in the PHR from the covered entity is covered under the HIPAA Privacy Rule, which, among other things, requires consent to disclose the PHI to the PHR vendor.

Routine big data analytical techniques can now effectively assemble personal data that is not protected by any of the laws currently in effect. In some cases, marketing initiatives have been successful without turning to protected health information. In one example, Google Flu Trends offered a model for following how flu spreads by analyzing search-engine queries.[21] Another well-known illustration of this is the way Target creatively collated scattered pieces of data about an individual's changes in shopping habits to predict the delivery date of pregnant shoppers — in order to target them with relevant advertisements through the use of "predictive analytics." Target's actions drew public attention when it sent coupons to a teenage girl, whose father did not know she was pregnant. While Target did not stop using predictive modeling techniques, it did alter its advertising strategy to this target audience.[22]

Just because certain health information in a particular context is not covered under HIPAA does not mean there are no regulatory compliance issues of concern. As noted, the information may be subject to the Family Educational Rights and Privacy Act. Moreover, the FTC is proactively working to address the privacy and security concerns that may arise in connection with the monetization of data outside the traditional health care delivery environment. The FTC has the ability to prohibit and take enforcement actions against unfair and deceptive practices, including the handling of PHI not covered under HIPAA.

In May 2014, the FTC held a workshop on dealing with the treatment of consumer generated and controlled health information. There was a general consensus among government, industry, and private sector representatives that such data is sensitive and confidential, although the rapid expansion in types and amounts of such data may call for new legal steps to protect it. More recently, the FTC held a workshop on big data, which addressed the regulatory gaps, among other issues.[23] In December 2014, the FTC entered into a consent order with PaymentsMD and its chief executive officer, based on charges that the company misled thousands of consumers who signed up for an online billing portal by failing to adequately inform them that the company would seek highly detailed medical information from pharmacies, medical labs, and insurance companies.[24] Thus, it seems likely that the FTC will continue to be proactive with respect to protecting consumer health data. Organizations should continue to monitor the FTC's activities in this area to maximize their ability to comply with the FTC's regulatory requirements and guidance.

Other federal laws may also apply to covered entities and business associates. Such laws include the federal confidentiality of substance abuse records statutes,[25] which protect patient records that are maintained by or in connection with a federally assisted drug or alcohol program; the Privacy Act of 1974,[26] which governs the privacy of information contained in a system of records

maintained by a federal agency (or its contractors); and the federal Clinical Laboratory Improvement Amendments (CLIA),[27] which regulate disclosure by laboratories. In addition, the Gramm-Leach-Bliley Act[28] and, in some cases, the Employee Retirement Income Security Act[29] may apply to covered entity health plans.

While HIPAA provides a baseline for federal health information privacy protection, it does not preempt contrary state laws or regulations that are more stringent than HIPAA with respect to the protection of the privacy of health information.[30] The result is a patchwork of different standards for data privacy. Although laws that govern medical or health information vary markedly from state to state, there are certain generalities that can be made. There is a small group of states with comprehensive and relatively stringent privacy schemes for governing health or medical information. These include California, Florida, Illinois, Maine, Massachusetts, New Hampshire, Tennessee, and Vermont. Almost all states have enacted laws that apply to specific categories of sensitive information, such as genetic information, HIV test results, substance abuse information, and mental health information. An overview of select, relevant state law is included at Appendices A and B, and are described in greater detail below.

The 50-state survey they describe was designed to provide an overview of applicable state law, limited to select state statutes. It did not address state administrative regulations, attorney general opinions, licensure board opinions, and court decisions — each of which may impact a state's privacy regime. In addition, state laws and regulations in this area are subject to frequent change. The survey should nonetheless serve as a useful overview of the legal landscape, for reference purposes only and not as legal advice.

FOLEY & LARDNER LLP

Key Federal Requirements for Big Data Types

As mentioned above, HIPAA is the key federal law governing PHI,[31] and prohibits the use or disclosure of PHI without individual authorization, except in limited circumstances defined in the Privacy Rule.

The HIPAA Privacy Rule also requires covered entities to make reasonable efforts to limit the PHI used, disclosed, or requested for any purpose other than in direct treatment, to the "minimum necessary" to accomplish the intended purpose of the use and disclosure, except in limited circumstances.[32] As discussed above, the Privacy Rule applies to "covered entities" and to the "business associates" of such covered entities, (i.e., any downstream subcontractors that provide financial, administrative, data transmission, and certain other services for, or on behalf of, covered entities, or on behalf of the business associates to such covered entities). Organizations that store or transmit PHI such as electronic health record (EHR) vendors and health information exchanges (HIE) are all considered "business associates" under these regulations.[33]

Information Collected From Covered Entities Without Individual Authorization

ANALYSIS FOR COVERED ENTITIES' HEALTH CARE OPERATIONS

There are several alternatives under HIPAA that allow for the sharing and aggregation of PHI without patient authorization. For example, two or more covered entities that participate in joint activities may share PHI about their patients in order to manage and benefit their joint operations as an organized health care arrangement (OHCA). In order to qualify as an OHCA, the legally separate covered entities must be clinically or operationally integrated and share PHI for the joint management and operation of the arrangement.[34] In addition, they must hold themselves out to individuals as an integrated system and inform individuals that they will share PHI for their joint operations.[35] Members of an OHCA are permitted to disclose PHI to other covered entity participants for the joint health care operations[36] activities of the OHCA without entering into business associate agreements.

The HIPAA Privacy Rule also allows business associates to aggregate PHI from multiple covered entities, or an OHCA, for health care operations purposes[37] of the covered entities with whom they contract. For example, accountable care organizations (ACOs) participating in the Medicare Shared Savings Program (MSSP) may permissibly aggregate and analyze data from multiple participants and providers, either in the capacity of business associates or covered entities, to improve health care quality and reduce costs. Such uses and disclosures, according to CMS, are considered "healthcare operations" purposes.[38] However, the HIPAA Privacy Rule does not permit the further use or disclosure of PHI by the business associate for secondary purposes unless the data are de-identified, as discussed below.

CREATION AND USE OF DE-IDENTIFIED DATA

As a result of the laws and regulations prohibiting the sharing or disclosure of PHI without patient consent, de-identification of PHI by covered entities or business associates — as permitted under the Privacy Rule — can be a useful tool for monetizing health information.

This approach permits unlimited secondary uses of information derived from PHI. There are two methods through which PHI may be de-identified under HIPAA: 1) the safe harbor method, which requires the removal of specified individual identifiers (described below) as well as an absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual, and 2) the expert determination method, which involves a formal determination by a qualified expert.[39] The safe harbor method requires removal of 18 identifiers of the individual or of relatives, employers, or household members of the individual, including names, all elements of dates (except year), and all geographic subdivisions except for the first three digits of a zip code, where the geographic unit contains more than 20,000 people. In addition, the covered entity must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.[40] An expert is a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable. The expert must determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information. Further, the expert must document the methods and results of the analysis that justify such determinations.[41]

In many cases, the expert determination method may be a better alternative to satisfy the de-identification standard because the current statistical methods allow for preservation of a greater number of data elements than under the safe harbor method. In particular, geographic data (e.g., zip codes) and dates (e.g., dates of service), which cannot be included in a data set that is de-identified under the safe harbor method, may permissibly be included in a data set that is de-identified under the expert determination method.

STRATEGIES FOR AGGREGATION AND DE-IDENTIFICATION OF PHI BY BUSINESS ASSOCIATES

To establish its ability to aggregate and de-identify PHI in compliance with HIPAA, a business associate should ensure that its business associate agreement addresses the following issues:

- The business associate agreement should expressly state that the business associate may aggregate PHI for the health care operations purposes of the covered entity (or OHCA, if applicable). This is important because a business associate is not permitted to use or disclose PHI for purposes other than those permitted by its business associate agreement or required by law.[42] The aggregation of PHI for health care operations is a permissible use of data by a business associate under HIPAA.[43] Therefore, a business associate may permissibly aggregate data to perform analysis for the health care operations of organizations that contribute data under a business associate agreement. For example, a business associate that conducts analysis for ACOs may aggregate data from all of the ACO-participant members and their providers for the analysis.
- The business associate agreement should also expressly permit the business associate to de-identify the information.[44] Under HIPAA, a business associate can only make secondary uses of aggregated data for purposes other than the health care operations of the covered entity if the business associate de-identifies the data or obtains patient authorization for such uses.[45] In many cases, obtaining patient authorization for proposed secondary uses may not be feasible. Upon de-identification of such information, the data is no longer considered PHI and thus not subject to HIPAA.

The data may therefore be analyzed, disclosed, or sold by the business associate without restriction.

» Finally, the business associate agreement should exclude de-identified data from any provisions that relate to the covered entity's ownership of the data, or it should include an express transfer of ownership interest in de-identified data.

MARKETING AND SALE OF PHI

The HIPAA Privacy Rule restricts the use and sharing of PHI for "marketing communications" and restricts the "sale" of PHI. A marketing communication is one that encourages the purchase of third-party products or services. Generally, if the communication is "marketing," then the communication can occur only if the covered entity first obtains the individual's authorization.

For example, a marketing communication would occur when a hospital informs former patients about a cardiac facility that is not part of the hospital, and the communication is not for the purpose of providing treatment advice. Similarly, a communication from a health insurer promoting a home and casualty insurance product offered by the same company would be a marketing communication.

Another type of marketing communication regulated by HIPAA occurs when a covered entity discloses PHI in exchange for financial remuneration from a third party seeking to make a marketing communication about the third party's own products or services. For example, a health plan selling a list of its members to a company that sells blood glucose monitors, which intends to send the plan's members brochures on the benefits of purchasing and using the monitors would be considered a marketing communication. As would a drug manufacturer receiving a list of patients from a health care provider and providing remuneration to the provider, then using that list to send discount coupons for a new anti-depressant medication directly to the patients.

Prior to enactment of the HIPAA Omnibus Rule in 2013, a covered entity could share PHI with a third party to make a marketing communication relating to treatment of the patient, even if the covered entity received compensation. This is no longer the case, as sharing of PHI for any purposes, including treatment, requires authorization if the covered entity receives any type of financial remuneration.

HIPAA contains an exception for reminders for refills for prescriptions, and for communications relating to the delivery of drugs and biologics, provided that the financial remuneration is reasonably related to the cost of making the communication. For example, if a patient self-administers a certain drug or biologic, PHI can be shared for the purpose of marketing communications about the drug delivery system, such as an insulin pump, can be sent without prior authorization provided the covered entity receives no profit in excess of the cost of making the communication. Thus, to the extent that a covered entity or business associate intends to use health information for marketing purposes, the strategy for collection and use should involve careful consideration of whether individual authorization is required to satisfy the requirements of HIPAA.

In addition to restrictions related to marketing communications, HIPAA restricts the "sale" of PHI in situations broader than marketing. If a covered entity proposes to engage in a sale of PHI (i.e., an exchange of PHI for a direct or an indirect remuneration), individual authorization is required, unless the sale falls within an exclusion. Unlike the marketing restrictions, remuneration for purposes of triggering a sale can be financial or non-financial, such as gifts in-kind. Additionally, a sale under the Rule is not limited to outright transfers of PHI, but also covers licenses and leases of PHI.

One exception to the sale rule applies if the sale is for public health purposes or research, as long as the payment is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI.[46] Additionally, PHI can be sold for treatment and payment purposes, and in connection with the merger or sale of a covered entity. Disclosures to business associates for health care operations, to patients and to health information exchanges also do not trigger the sale restrictions.

If authorizations for "sale of PHI" are obtained from individuals, such authorizations must state that remuneration for the PHI is involved.[47] If PHI is properly "sold" to a third party pursuant to an authorization or permitted use under one of the exceptions set forth above, and the third party is not subject to HIPAA, there are no restrictions on how the third party may further use, disclose, or sell the data. However, if the third party is subject to HIPAA as a covered entity, then the third party must continue to abide by the HIPAA Privacy Rule's restrictions on use or disclosure of any PHI that it creates or receives. For example, if a data set containing PHI is "sold" to a data analytics company with patient authorization, the data is no longer subject to HIPAA's restrictions because such companies are not covered entities that are governed by HIPAA. On the other hand, if PHI is "sold" with patient authorization to a health care provider, the health care provider can only use and disclose such PHI in accordance with HIPAA.

Although sale of identifiable PHI is prohibited under HIPAA without individual authorization, sale of de-identified data has been held to be permissible in the limited number of state court cases regarding this legal issue. In one case, the state court upheld the defendant provider's motion to dismiss, ruling that the HIPAA Privacy Rule does not restrict the use or disclosure of de-identified information because it is not PHI.[48]

CREATION OF RESEARCH DATABASES FOR FUTURE RESEARCH USES OF PHI

Research is another area where health information can be monetized. Research databases often include clinical information or claims information created and maintained by covered entities. Such databases and their content are subject to the HIPAA Privacy Rule. The Privacy Rule provides several key "pathways" that permit use of PHI to create research[49] databases for future research purposes:

- **Collection and Use of a Limited Data Set.** This may include geographic information other than street address, all elements of dates and ages, and certain other unique identifying characteristics or codes. A covered entity may release a limited data set if the researcher signs a data use agreement (DUA), which assures the covered entity that the recipient will protect the limited data set and will not make any effort to re-identify individuals using the data set.[50]
- **Collection and Use of De-Identified Data.** Discussed above.[51]
- **Pursuant to an Institutional Review Board (IRB) or Privacy Board Waiver of Authorization.** An IRB operating under a federal-wide assurance, or a privacy board that functions under the Privacy Rule, may grant a waiver or alteration of the written authorization if the proposed use or disclosure will pose minimal risk to participants' privacy, the research could not practicably be conducted without the waiver or alteration of authorization and it cannot be conducted using de-identified information, and other specified criteria are met.[52]
- With authorization from the individual to create the research repository.[53]

TABLE 1 **HIPAA Pathways for Research Databases**

	Limited Data Set With DUA	De-Identified Data Set	Waiver of Authorization	Authorization/Consent
Advantages	No subject authorization or consent required. May be useful for health services research and related studies.	No subject authorization or consent required. Unlimited uses and disclosures permitted for any purpose. May commercialize data or results of analysis.	No subject authorization or consent required.	May permit use for future unspecified research uses and commercialization of research results. HIPAA minimum-necessary standard does not apply.
Disadvantages	DUA may restrict further uses and disclosures, the length of time the data are available, and the ability to link with other data sets. Limited data set includes only a few more elements than de-identified data, so its research uses may be limited.	De-identification of data limits its research uses, and is not useful for certain clinical and studies.	Requires the involvement of the IRB or privacy board. IRB or privacy board may not approve in cases where it would be feasible to request authorization from the individuals who are the subject of the information.	Requires interaction with individual subject of the information.

The table above illustrates the advantages and disadvantages of these approaches.

According to the U.S. Department of Health and Human Services (HHS), the development of research repositories and databases for future research purposes is itself a "research activity," thereby requiring authorization or waiver of authorization to the extent PHI would be involved. Prior to the recent enactment of the Omnibus HIPAA Final Rule, the HIPAA Privacy Rule did not allow covered entities to use or disclose PHI for the creation of research databases of PHI for future unspecified research. Instead, the law required individual authorizations for each specific study. To facilitate secondary research activities using databases or data repositories, HHS recently reversed this policy.[54] The revised HIPAA Privacy Rule allows covered entities to obtain individual authorization for the uses and disclosures of PHI for future research purposes, so long as the authorization adequately describes the future research such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for future research purposes.[55] The revised Privacy Rule also provides considerable flexibility regarding 1) a description of the PHI to be used and 2) a description of the recipients of the PHI (which may be unknown) for the future research.[56]

Much of the biomedical and behavioral research conducted in the United States is also governed either by the rule entitled "Federal Policy for the Protection of Human Subjects" (also known as the "Common Rule"[57]) and/or the U.S. Food and Drug Administration's (FDA) Protection of Human Subjects regulations.[58] These human subjects regulations apply to federally funded and some private research activities.[59] Similar to the revised HIPAA requirement, these federal human subjects protection regulations require informed consent of the research participant for the creation of research databases and repositories; informed consent documents must, among other requirements, include an "explanation of the purposes of the research."[60] This requirement has been interpreted to permit researchers to collect specimens and data for future research whose specific purposes may be unknown. For example, the National Cancer Institute informs potential participants that their tissue may be used in all types of research, such as finding the causes of disease, developing new tests or new drugs, and genetic research, and that they have no right to decide the type of research in which their tissue is used.[61]

Although federal human subjects protections do not directly govern private research databases, they regulate the activities of researchers who may ultimately use the research repository to conduct

particular studies. In cases where informed consent was not obtained, the use of such data by federally funded research studies could be compromised. To optimize the value of private research databases to researchers and to ensure maximum flexibility of use for future research, informed consent for creation of the database and future research uses should be requested in concert with the request for authorization under HIPAA.

Health Information Collected From Individuals

PERSONAL HEALTH RECORD (PHR)

PHRs offer additional monetization alternatives. Although HIPAA and the HITECH Act have increased the restrictions on the use and disclosure of PHI, the increased ability of health care organizations to effectively and efficiently aggregate patient health records obtained directly from patients is acting to counterbalance regulatory restrictions. For example, even though a PHR offered to a patient by a vendor (such as Microsoft HealthVault or WebMD Health Manager) may contain the same information as a PHR offered by a covered health care provider (e.g., a hospital that provides a patient portal to a PHR), the PHR is not subject to the same legal requirements because the PHR vendor is not a covered entity that is governed by HIPAA.

In general, a PHR is an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in his or her own health care. HHS clarifies that the HIPAA Privacy Rule applies solely to PHRs that are offered by health plans or health care providers that are covered by the HIPAA Privacy Rule, but not to those offered by employers (separate from the employer's group health plan) or by PHR vendors directly to an individual are not subject to HIPAA.

PHR vendors are governed by the privacy policies of the entity offering them and are subject to the jurisdiction of the FTC.[62] FTC regulations have established health breach reporting obligations and applied these requirements to PHR vendors (online services that allow consumers to organize and store medical information from many sources), PHR-related entities that offer products through the vendor's website or access or send information to a PHR (such as web-based applications that that allow patients to upload reading from a blood pressure pedometer into a PHR), or third-party service providers to vendors of PHRs. The FTC treats violation of the breach reporting regulation as an unfair or deceptive act or practice.[63]

Even though HIPAA does not directly regulate PHR vendors, PHR-related entities, or third-party service providers, the HIPAA Privacy Rule does regulate the disclosure of an individual's PHI by a HIPAA covered entity to such entities. Therefore, in cases whether the PHR is populated by a covered entity, a HIPAA compliant authorization from the individual who is the subject of the information must be obtained. Typically, a PHR vendor, PHR-related entity, or third-party service provider will request such authorization as part of the patient's registration for the services. The authorization may be executed electronically, provided any electronic signature obtained from the individual complies with applicable law.[64] Alternatively, a covered entity may provide the record to the individual for the individual to enter into his or her PHR.[65]

MOBILE TECHNOLOGIES AND WEB-BASED APPLICATIONS

If data is gathered from consumers through a web-based application or mobile device that does not interface with a PHR, the information is outside the scope of both HIPAA and the FTC breach reporting regulations. In 2014, the FTC held a series of forums to address privacy issues related to: 1) mobile device tracking — tracking consumers in retail and other businesses using signals from their mobile devices; 2) alternative scoring products — using predictive scoring to determine consumers' access to products and offers; and 3) consumer-generated and controlled health data — information provided by consumers to non-HIPAA covered websites, health applications, and devices.[66] Absent a change in the law, data housed through websites, such as PatientsLikeMe, are governed only by the business' privacy policy and applicable state law.

In addition to the wealth of new health data generated by health applications and devices, the increased use of social networking tools such as Facebook, mobile tracking devices, and applications that put personal information in the public domain provides greater analytic capacity with fewer regulatory protections. As the Target and Google examples previously discussed illustrate, when businesses that are not subject to health data laws create or maintain sensitive health information, their privacy policy and practices for use of the data should reflect a thoughtful consideration of the consumers' expectations.

STRATEGIES FOR MANAGING HEALTH DATABASES

To maximize their ability to engage in monetization activities, organizations that collect, access, or host health data — including PHR vendors, providers of web-based applications, and their third-party providers — are best advised to create and implement a privacy policy designed to comply with applicable laws and implement "best practices" regarding use of collected data. Any such policy should establish the organization's uses and disclosures of individual health records and related personally identifiable information. The organization should ensure that an individual using its service reads and agrees to the privacy policy. If health information is collected directly from individuals for future research purposes, the entity should consider obtaining informed consent from the individual to enhance the viability of future research uses of the data.

FOLEY

FOLEY & LARDNER LLP

Key State Laws Limiting the Use of Health Information

Unlike HIPAA, state laws may affect the ability to do one or more of the following without individual consent: disclose individually identifiable health information without consent for purposes other than treatment; use health information for research; and/or make any secondary use of certain sensitive information. The framework they create is complex and often conflicting. It has been colorfully labeled a "patchwork quilt" of privacy protection.[67]

Overview of State Big Data Requirements

A very limited number of states, including Hawaii, Iowa, Kansas, Missouri, Ohio, and West Virginia, have worked to comprehensively harmonize their state statutory regime with HIPAA. Other state laws may allow that compliance with HIPAA constitutes compliance with the state statute, regardless of any facial conflict. However, in general, states vary as to how they protect sensitive health information, the information protected, the entities covered by applicable requirements, and the ability to disclose or redisclose information. The result is a panoply of complex and conflicting requirements for businesses operating across state lines. Although it is difficult to summarize easily applicable state requirements, there are several guiding principles that can be observed.

A limited number of states have created a statutory right to privacy, vesting individuals with broad ownership rights of their health information. Massachusetts, for example, has a patient bill of rights, under which every patient or resident of a hospital or other facility shall have the right to confidentiality of all records and communications to the extent provided by law.[68] A violation of this Massachusetts statute may result in a civil action, although to date Massachusetts courts have not interpreted the statute in the health information context. New Hampshire's equivalent law provides that the patient shall be ensured confidential treatment of all information contained in the patient's personal and clinical record, including that stored in an automatic data bank, and the patient's written consent shall be required for the release of information to anyone not otherwise authorized by law to receive it.[69] Tennessee and Vermont have adopted similar broad protections.

A more common approach is to restrict disclosure of PHI by providers (or categories of licensed institutions or professionals), insurers, managed care organizations or health maintenance organizations (HMOs), or others, without individual authorization, unless a specific exception allowing such disclosure is satisfied. For example, most states create additional personal ownership rights in certain categories of health information, such as genetic information, HIV test results, communicable disease, substance abuse information, and/or mental health information.

State privacy laws also may apply to entities other than those covered by HIPAA. This means that an entity that is not regulated by HIPAA may still be subject to state privacy laws with respect to the individually identifiable health information that it maintains. For example, California deems "any business organized for the purpose of maintaining medical information" to make such information available to an individual (for the purposes of managing his or her own health care) or to a health care provider (for the diagnosis or treatment

TABLE 2 **Sample State Provisions Governing Disclosure/Use of PHI in Research**

	Statutory Construct	State/Citation	States With a Similar Construct
Research — De-Identified Data	Permissive disclosure in connection with use in actuarial or research studies, provided: 1) no individual is identified; 2) materials in which the individual may be identified are returned or destroyed; and 3) the organization agrees not to further disclose the information	Conn. Gen. Stat. § 38a-988 (2012) (applicable to insurance institutions, agents, and insurance-support organizations)	Connecticut, Florida, Illinois, Massachusetts, Minnesota, New Jersey, North Carolina, Tennessee, Wisconsin
Research — Waiver of Authorization (Privacy Board)	PHI may be disclosed for research, with approval or waiver of the applicable privacy board in accordance with HIPAA, subject to a finding of 1) no more than a minimal risk to privacy of individuals, based on, at least, an adequate plan to protect the identifiers from improper use and disclosure, to destroy the identifiers at the earliest opportunity, and adequate written assurances that the PHI will not be reused or further disclosed except as permitted; 2) the research could not practicably be conducted without the waiver or alteration; and 3) the research could not practicably be conducted without access to and use of the PHI.	Del. Code Tit. 16 § 1212	California, Delaware, Maine, Maryland, Washington, Wyoming

of an individual) as a "provider of healthcare" with regards to the confidentiality standards established in the California Medical Information Act (CMIA).[70] The law applies to "medical information" disclosed to the business. The term "medical information" means any "individually identifiable" information regarding a patient's medical history, mental or physical condition, or treatment.[71] The *primary* purpose of the business need not be the maintenance of medical information; it merely has to be one of the purposes of the business. Therefore, arguably, this law has broad applicability to PHR vendors and other businesses with web-based consumer-facing applications — activities that may be subject to lesser regulation under federal law.

Research provides a good example of how state requirements may overlap, but not be entirely consistent with, federal laws. Several states have adopted statutes that allow the use of confidential health information in research and actuarial studies by insurance companies, agents, and support organizations, provided that there are sufficient privacy safeguards in place. Other states have adopted provisions regarding use of confidential health information in research that are consistent with federal provisions requiring IRB or privacy board authorization. Illustrations of such laws are below. Outside of states that have provided for use of health data consistent with HIPAA, state laws specifically authorizing the use of limited data sets are rare. A particular note of caution applies, however, in connection with research that may rely on specific categories of PHI. In this regard, some states, such as Minnesota, do not allow disclosure unless the researcher makes reasonable attempts to obtain patient authorization.[72] In any event, the diversity of state law should be given careful consideration in any design of a research database or repository. The above table illustrates some of the relevant state law provisions referenced in the attached appendices.

Several states expressly restrict the ability to sell health information. These laws may be applicable to providers, insurers, HMOs, or more broadly. Connecticut, for example, requires that insurance institutions, agents, and insurance-support organizations meet a specific exception to disclose privileged information concerning an individual. There is an exception available in connection with the marketing of a product or service, provided: 1) no medical record information, privileged information, or personal information relating to an individual's

character, personal habits, mode of living, or general reputation (or classification derived from such information) is disclosed; 2) the individual has the opportunity to opt out; and 3) the person receiving such information agrees not to use it except in connection with the marketing of a product or service.[73] As noted in Table 3 below, this construct is similar to applicable laws in Arizona, California, Maine, Massachusetts, New Jersey, and North Carolina. On the other hand, certain provider-focused statutes (such as those in New Hampshire, Montana, Oregon, and Washington) regulate the use of "medical information" for marketing without individual authorization more stringently.[74] If an entity subject to such state's law will receive remuneration from a third party (such as a drug or device manufacturer), it should obtain legal review of its proposed strategy for use of the information. The following table provides examples of the various state law provisions applicable to sales and marketing initiatives.

based consumer facing application maintains medical information, any individual authorization the business may seek in connection with proposed uses of such data should be designed to comply with state law specific requirements.

State Law Compliance Strategies

In light of the U.S. regulatory scheme governing the privacy of individually identifiable health information, businesses that are considering monetization of health data should map the flow of data and the type of data to develop appropriate, legally compliant strategies that would facilitate any potential or proposed secondary uses of such data. Strategies should address authorization and consent for prospective uses of data received from covered entities, business associates, other entities subject to state law, or individuals. If data is collected directly from individuals, then the data collector's use and subsequent disclosure of such information will likely not be

TABLE 3 **Sample State Provisions Governing Disclosure/Use of PHI in Sales/Marketing**

	Statutory Construct	State/Citation	States With a Similar Construct
Sales/Marketing — Baseline Approach	Disclosure permissible if: 1) no information relating to an individual's character, personal habits, mode of living, or general reputation is disclosed and no classification derived from the information is disclosed; 2) the individual has been given an opportunity to opt out; and 3) the person receiving the information agrees not to use it except in connection with the marketing of a product or service.	AZ Rev. Stat. Ann. § 20-2113 (2012) (applies to insurance institutions, insurance producers and insurance support organizations)	Arizona, California, Connecticut, Maine, Massachusetts, New Jersey, North Carolina
Sales/Marketing — More Stringent Approach	Release or use of patient identifiable medical information for the purpose of sales or marketing of services or products shall be prohibited without written authorization.	N.H. Rev. Stat. Ann. § 332-I:1, 3	New Hampshire, Montana, Oregon, Washington

Finally, certain states delineate specific requirements for what would constitute valid individual authorization for the use and disclosure of health information. In California, for example, the CMIA authorization requirements are consistent with HIPAA, except they require that patient authorization forms to be a typeface that is no smaller than 14-point type.[75] Therefore, to the extent that a business such as a web-

restricted by HIPAA or other federal regulations. Nevertheless, such businesses may still be subject to state law, either if a state law applies directly to businesses that maintain medical information or if a state law governs a person who obtains certain sensitive health information. Therefore, the proposed uses of or ability to redisclose protected information may be restricted. For example, if the information

includes genetic information, informed consent regarding the commercialization of the data, and data ownership should be addressed.

Common sense privacy safeguards are also advisable. If a business operates across state lines, identifying any states with more stringent requirements, and incorporating those state standards into the business's compliance policies is also recommended. In addition, a best business practice would be to provide a general notice to patients that any personal information gathered through treatment may be used in de-identified form in analytic models. Such practical steps should be designed to enable people to understand how and why their data is being used, and inform them of the risk of data breach.

FOLEY

FOLEY & LARDNER LLP

Despite Regulatory Challenges, Big Data Is Worth It

Although the government is working to incentivize the use of technology, and promote transparency and access to data, federal and state regulators are not generally perceived as keeping pace with technological advances.

There is a fear that this in turn can stifle innovation, with cash-strapped start-up companies lacking financial resources needed to navigate the myriad laws and regulations applicable to their products and services.[76] This does not need to be the case. A carefully designed compliance program and ongoing monitoring of the legal landscape can help a company navigate the legal and regulatory framework to successfully monetize health care data.

FOLEY

FOLEY & LARDNER LLP

About the Authors

For more information about monetizing health care-related Big Data and the corresponding regulations, contact your Foley attorney or any of the following authors and contributors.

Authors

C. Frederick (Fred) Geilfuss II
Milwaukee, Wisconsin
414.297.5650
fgeilfuss@foley.com

M. Leeann Habte
Los Angeles, California
213.972.4679
lhabte@foley.com

Chanley T. Howell
Jacksonville, Florida
904.359.8745
chowell@foley.com

Adria Warren
Boston, Massachusetts
617.342.4092
awarren@foley.com

Contributors

R. Michael (Mike) Scarano, Jr.
San Diego, California
858.847.6712
mscarano@foley.com

Melesa A. Freerks
Chicago, Illinois
312.832.5158
mfreerks@foley.com

Lindsey E. Gabrielson
Boston, Massachusetts
617.502.3285
lgabrielsen@foley.com

Adam J. Hepworth
Los Angeles, California
213.972.4604
ahepworth@foley.com

Patrick O. Hernon
Boston, Massachusetts
617.342.4067
phernon@foley.com

Asha M. Natarajan
New York, New York
212.338.3639
anatarajan@foley.com

Elizabeth J. (Betsy) Rosen
New York, New York
212.338.3623
erosen@foley.com

Taylor E. Whitten
Chicago, Illinois
312.832.5764
twhitten@foley.com

---

[1] V. Greenwood, "Dr. Data," *The New York Times Magazine* (October 5, 2014).
[2] McKinsey & Company, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (May 2011), http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.
[3] McKinsey & Company, *The "Big Data" Revolution in Healthcare* (January 2013), http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.
[4] HealthIT Dashboard. Hospitals receiving incentive payments for electronic health record adoption or

meaningful use: May 2011 to Dec 2013. HealthIT Quick-stat [serial on the internet]. 2014 Feb [cited 2014 May 16]. Available from: http://dashboard.healthit.gov/quickstats/PDFs/Health-IT-Quick-Stat-Hospitals-Receiving-Payments-for-MU-and-Adoption.pdf.

[5] See Sept 19, 2014, *The Wall Street Journal*, "Two Ways Big Data is Reshaping Healthcare" by Drew Harris.

[6] See Aug 22, 2014, *The Wall Street Journal*, "Can Big Data Improve Medical Diagnoses?" Elizabeth Dwoskin.

[7] Brian Denton "Commentary: Health system CIOs can access a wealth of data on the use of precious resources, from clinicians to MRI machines. Here are specific steps to start using that data better." *Information Week*, June 5, 2014.

[8] Aug. 13, 2014, *The Wall Street Journal*, "Intel Tries to Tackle Tough Disease with Big Data" by Elizabeth Dwoskin.

[9] Id.

[10] *Transparency and Open Government*, Memorandum of President Obama for Heads of Executive Departments and Agencies (January 21, 2009).

[11] *Freedom of Information Act*, Memorandum of President Obama for the Heads of Executive Departments and Agencies (January 21, 2009).

[12] Wendy R. Ginsberg, *Congressional Research Service. The Obama Administration's Open Government Initiatives Issues for Congress* (January 28, 2011); John Wonderlich, *Obama's Open Government Directive, Two Years On*, Sunlight Foundation Blog (December 7, 2011).

[13] Obama Administration Unveils "Big Data" Initiative, Release of the Office of Science and Technology Policy (March 29, 2012)

[14] Id.

[15] National Science Foundation, Press Release 12-187 (October 3, 2012)

[16] Id.

[17] Id.

[18] Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996.

[19] 45 C.F.R. §160.103. PHI is defined to include individually identifiable health information that 1) is *created or received by covered entities*, i.e., health plans, health care clearinghouses, and certain health care providers that engage in standard electronic administrative and financial transactions regulated by HIPAA ("covered health care providers"), such as claims submission or health plan enrollment, and 2) that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual (including demographic information), and 3) that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

[20] U.S. Department of Health and Human Services (HHS), *Personal Health Records and the HIPAA Privacy Rule*, available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

[21] *Nature* reported that in 2013, Google estimated almost twice as many flu cases as the Centers for Disease Control and Prevention estimated.

[22] Forbes, "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did" (Feb. 16, 2012).

[23] FTC, *Big Data: a Tool for Inclusion or Exclusion* (Sept. 15, 2014) available at http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

[24] FTC, PaymentsMD LLC in the Matter of, available at http://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter.

[25] 42 U.S.C. §290-dd and its implementing regulations at 42 C.F.R. Part 2.

[26] 5 U.S.C. §552a *et seq.*

[27] 42 U.S.C. §263a, 42 C.F.R. Part #?

[28] 15 U.S.C. § 5801 *et seq.*

[29] 29 U.S.C. §1002 *et seq.*

[30] 45 C.F.R. § 160.203.

[31] 45 C.F.R. §160.103; Protected health information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

[32] 45 C.F.R. §164.502(d).

[33] 45 C.F.R. §160.103. Note that a covered entity may also serve as a business associate.

[34] 45 C.F.R. §164.506(c)(5).

[35] 45 C.F.R. §164.520(d).

[36] "Health care operations" are 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. These activities, which are limited to the activities listed in the definition of "health care operations" at 45 C.F.R. 164.501, include: conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims; conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. 45 C.F.R. §164.506.

[37] Covered entities may disclose PHI to for their own health care operations, or may disclose PHI to another covered entity for certain health care operation activities of the entity that receives the information if 1) each entity either has or had a relationship with the individual who is the subject of the information, and the PHI pertains to the relationship; and 2) the disclosure is for a quality-related health care operations activity or for the purpose of health care fraud and abuse detection or compliance.[37]

[38] U.S. Department of Health and Human Services (HHS), Medicare Program; Medicare Shared Savings Program: Accountable Care Organizations; Final Rule, 76 Fed. Reg. 67802 (Nov. 2, 2011).

[39] 45 C.F.R. §164.514(a)-(b). It is important to know that the Privacy Rule permits a covered entity to assign to, and retain with, the de-identified health information, a code or other means of record re-identification if that code is not derived from or related to the information about the individual and is not otherwise capable of being translated to identify the individual. For example, an encrypted individual identifier (e.g., a Social Security Number) would not meet the conditions for use as a re-identification code for de-identified health information because it is derived from individually identified information. In addition, the covered entity may not 1) use or disclose the code or other means of record identification for any purposes other than as a re-identification code for the de-identified data, and 2) disclose its method of re-identifying the information.

[40] 45 C.F.R. § 164.514(b)(2).

[41] HHS, Office for Civil Rights (OCR), *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, available at http://www.gpo.gov/fdsys/pkg/FR-2011-11-02/pdf/2011-27461.pdf.

[42] 45 C.F.R. §164.504(e)(2)(ii)(A).

[43] 45 C.F.R. §160.103.

[44] *See,* OCR, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*.

[45] 45 C.F.R. §164.502(a).

[46] 45 C.F.R. §164.502(a)(5)(ii); other permissible purposes are treatment and payment; a sale and merger transaction involving the covered entity or the business associate; activities performed by a business associate for or on behalf of the covered entity (or by a business associate subcontractor for or on behalf of the business associate) if the payment is for the business associate's performance of such activities (or for the subcontractor's performance of such activities); providing an access or an accounting to an individual; as required by law; and as otherwise permitted under HIPAA, where only a reasonable, cost-based fee is paid (or such other fee as permitted by law). Although this last exclusion is not well defined, it involves situations where authorization from the individual is received and where patient information is aggregated and de-identified, discussed above.

[47] 45 C.F.R. §164.508(a)(4).

[48] *Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331, 338 (E.D. Pa. 2012).

[49] Both the Common Rule and HIPAA define research as a "systematic investigation…designed to develop or contribute to generalizable knowledge."
[50] 45 C.F.R. §153.512(i).
[51] 45 C.F.R. §153.502(d).
[52] 45 C.F.R. §153.512(i).
[53] 45 C.F.R. §164.508.
[54] HHS, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, Final Rule, 78 Fed. Reg. 5566 (Jan. 25, 2013).
[55] HHS, OCR, Research, available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/research.html.
[56] For studies that began prior to March 26, 2013, covered entities and researchers may permissibly rely on an IRB-approved consent that reasonably informed individuals of the future research, even though the HIPAA authorization relates (as was required) only to a specific study; *see,* HHS, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566, 5612 – 5613 (Jan. 25, 2013).
[57] 45 C.F.R. Part 46, Subpart A.
[58] 21 C.F.R. Parts 50 and 56.3.
[59] The FDA regulations apply only to research over which the FDA has jurisdiction, primarily research involving investigational products; the Common Rule applies primarily to federally funded research or research at academic or other institutions that have an agreement to comply with the Common Rule.
[60] National Institutes of Health, National Cancer Institute, *Providing Your Tissue for Research*, available at http://www.cancer.gov/clinicaltrials/learningabout/providingtissue.
[61] Under the Privacy Rule, neither blood nor tissue, in and of itself, is considered individually identifiable health information; therefore, research involving only the collection of blood or tissue would not be subject to the Privacy Rule's requirements. However, to the extent that blood and tissue are labeled with information (e.g., admission date or medical record number) that the Privacy Rule considers individually identifiable and thus, PHI. A covered entity's use or disclosure of this information for research is subject to the Privacy Rule. In addition, the results from an analysis of blood and tissue, if containing or associated with individually identifiable information, would be PHI. *See,* HHS, National Institutes of Health, Research Repositories, Databases, and the HIPAA Privacy Rule, available at http://privacyruleandresearch.nih.gov/research_repositories.asp. Note, however, that tissue banking may be subject to state tissue banking laws, the Uniform Anatomical Gift Act, and FDA regulations that establish specific requirements.
[62] OCR, Personal Health Records and the HIPAA Privacy Rule.
[63] 16 C.F.R. §318 *et seq.;* PHR-related entities include entities that interact with a vendor of personal health records either by offering products or services through the vendor's website or by accessing information or transmitting information to a PHR. Many businesses that offer web-based apps for health information fall into this category.
[64] 45 C.F.R. §164.502(a)(1)(i).
[65] OCR, Personal Health Records and the HIPAA Privacy Rule.
[66] FTC, Spring 2014 Privacy Series, available at http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data, http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking, and http://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.
[67] Boyle, Lisa M., *A Guide to Healthcare Privacy*. (Wolter Kluwer's Law and Business: last updated Nov. 2013).
[68] M.G.L. 111 §70E.
[69] N.H. REV. STAT. ANN. §151:21.
[70] Cal. Civil Code §56.06.
[71] Cal. Civil Code §56.05(f); "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual (such as the patient's name, address, electronic mail address, telephone number, or Social Security Number), or other information that reveals the individual's identity.

[72] Minn. Stat. §144.2219 (applicable to studies approved by the commissioner that require identifying information about a child or a parent or legal guardian of the child).
[73] See, e.g., Conn. Gen. Stat. §38a-988 (2012).
[74] See, e.g., N.H. Rev. Stat. Ann. §332-I:1, 3.
[75] Cal. Civil Code §56.11.
[76] See, e.g., Christina Farr, "App Developers Seek Clearer U.S. Health Data Privacy Guidelines," *Reuters Business Insider* (Sept. 15, 2014) September 2014 (consortium of mobile-health startups seeks greater clarity and developer-friendly only resources around HIPAA).

FOLEY

FOLEY & LARDNER LLP

Appendix A — Overview of State Legal Framework

* Only select statutes and regulations have been included, and do not reflect a complete record of applicable state law. Information provided is for reference purposes only and not for legal advice, nor does it substitute for independent review of applicable state law. Foley & Lardner LLP makes no representation regarding the accuracy or completeness of the information included herein.

State	Right to Privacy or Other Restrictions on Disclosure				Use of Data in Research		Marketing and Sales		Specific Categories Protected					
	General or Comp-rehensive Provisions	Provider Specific Provisions	Insurer Specific Provisions	HMO Specific Provisions	Consent or De-Identification Required	Pursuant to Regulatory Board Approval	Providers	Insurers/ HMOs	Genetic Data	Cancer Status	Mental Health	Substance Abuse	Immun-ization Data	Birth Defects/ Disability
Alabama				√					√	√	√			
Alaska					√	√			√					
Arizona	√		√	√		√		√	√		√		√	
Arkansas		√	√	√					√					
California	√	√	√			√			√	√	√	√	√	
Colorado			√	√					√		√		√	
Connecticut		√	√	√	√		√	√		√		√		
Delaware	√	√				√			√		√	√		

FOLEY

FOLEY & LARDNER LLP

State	Right to Privacy or Other Restrictions on Disclosure				Use of Data in Research		Marketing and Sales		Specific Categories Protected					
	General or Comp-rehensive Provisions	Provider Specific Provisions	Insurer Specific Provisions	HMO Specific Provisions	Consent or De-Identification Required	Pursuant to Regulatory Board Approval	Providers	Insurers/ HMOs	Genetic Data	Cancer Status	Mental Health	Substance Abuse	Immun-ization Data	Birth Defects/ Disability
District of Columbia		√		√					√		√	√		
Florida	√	√			√				√		√	√	√	
Georgia		√		√					√	√	√	√	√	√
Hawaii	√								√					
Idaho		√		√					√	√	√			
Illinois	√		√	√	√				√		√	√		
Iowa		√		√						√	√	√		√
Iowa	√	√	√	√					√		√	√		
Kansas		√		√					√	√	√	√	√	
Kentucky			√	√					√		√	√		√
Louisiana			√	√										
Maine	√	√	√	√		√		√	√		√	√		√
Maryland	√	√	√			√			√	√	√	√		
Massachusetts	√	√	√	√	√			√	√	√	√	√		√
Michigan			√	√					√		√	√		

FOLEY

FOLEY & LARDNER LLP

State	Right to Privacy or Other Restrictions on Disclosure				Use of Data in Research		Marketing and Sales		Specific Categories Protected					
	General or Comp-rehensive Provisions	Provider Specific Provisions	Insurer Specific Provisions	HMO Specific Provisions	Consent or De-Identification Required	Pursuant to Regulatory Board Approval	Providers	Insurers/ HMOs	Genetic Data	Cancer Status	Mental Health	Substance Abuse	Immun-ization Data	Birth Defects/ Disability
Minnesota	√		√	√					√		√	√	√	
Mississippi			√	√										
Missouri		√							√		√		√	
Montana	√	√	√	√				√	√					
Nebraska		√	√	√					√					
Nevada				√			√	√	√					
New Hampshire	√	√	√	√			√	√	√		√	√		
New Jersey	√	√	√	√					√		√	√	√	
New Mexico		√		√	√				√		√	√		
New York		√	√	√					√		√		√	
North Carolina			√	√					√	√	√		√	
North Dakota			√	√										
Ohio	√		√						√	√	√	√		
Oklahoma			√						√					
Oregon	√	√	√					√	√					

FOLEY

FOLEY & LARDNER LLP

State	Right to Privacy or Other Restrictions on Disclosure				Use of Data in Research		Marketing and Sales		Specific Categories Protected					
	General or Comp-rehensive Provisions	Provider Specific Provisions	Insurer Specific Provisions	HMO Specific Provisions	Consent or De-Identification Required	Pursuant to Regulatory Board Approval	Providers	Insurers/ HMOs	Genetic Data	Cancer Status	Mental Health	Substance Abuse	Immun-ization Data	Birth Defects/ Disability
Pennsylvania			√	√					√					
Rhode Island	√	√		√					√					
South Carolina		√	√	√					√		√	√		√
South Dakota				√					√		√	√	√	
Tennessee		√		√			√	√	√	√	√	√	√	
Texas		√	√	√					√	√	√	√		√
Utah			√	√					√					
Vermont	√	√	√						√		√		√	
Virginia	√	√	√	√										
Washington		√	√		√	√			√		√	√		
West Virginia														
Wisconsin	√	√	√						√	√	√	√		
Wyoming		√	√	√		√			√		√	√		

FOLEY

FOLEY & LARDNER LLP

Appendix B — Select State Laws Governing Use and Disclosure of Health Data

* Only select statutes and regulations have been included, and do not reflect a complete record of applicable state law. Information provided is for reference purposes only and not for legal advice, nor does it substitute for independent review of applicable state law. Foley & Lardner LLP makes no representation regarding the accuracy or completeness of the information included herein.

State	Statue (Citation)	Title of Statute	Comments
Alabama			No general/comprehensive prohibition on disclosure of medical information.
	Ala. Code §27-21A-25	Confidential Information (under Chapter 21A Health Maintenance Organizations)	Restricts disclosure of health information by HMOs.
	Ala. Code §§ 34-26-2, 34-8A-21	Confidential relations between licensed psychologists, licensed psychiatrists, or licensed psychological technicians and their clients — Other statutory exclusions; Privileged communications	Right of confidentiality in mental health records.
	Ala. Code §§ 22-13-33, 22-13-34, 22-11A-14, 22-11A-22	Information to be confidential	Governs disclosure in connection with specific medical conditions (cancer, sexually transmitted diseases, mandatory tuberculosis reports submitted to health agencies).

State	Statue (Citation)	Title of Statute	Comments
Alaska			No general/comprehensive prohibition on disclosure of medical information.
	Alaska Stat. §08.29.200, 08.86.200	Licensed Professional Counselors - Confidentiality of communications; Psychologists and Psychological Associates — Confidentiality of communications	Health care provider-patient privileges. HMO confidentiality of medical information statute repealed.
	Alaska Stat. §47.30.590, 47.30.845	Welfare, Social Services and Institutions — Mental Health	Right of confidentiality in mental health records.
	Alaska Stat. §18.13.010	Genetic Privacy — Genetic testing	Genetic tests may not be performed and the results may not be disclosed without informed written consent.
	Alaska Stat. §18.05.042	Administration of Public Health and Related Laws — Access to health records	Data on birth defects, cancer, and infectious diseases that must be reported to the department of health are confidential (but may be used for research).
Arizona	Ariz. Rev. Stat. Ann. §§ 12-2292 through 12-2294, 36-509 (2012)	12-2292 Confidentiality of medical records and payment records 12-2293 Release of medical records and payment records to patients and health care decision makers 12-2294 Release of medical records and payment records to third parties 36-509 Confidential records; immunity (effective January 1, 2015)	Under Arizona law, all medical records and payment records, and the information contained in medical records and payment records, are privileged and confidential.

State	Statue (Citation)	Title of Statute	Comments
	Ariz. Admin. Code § R9-1-302 (2012)	Medical Records or Payment Records Disclosure	Rule allows for disclosure at the direction of the Human Subjects Review Board, if the medical records or payment records are sought for research and the disclosure meets the requirements of 45 CFR 164.512(i)(2).
	Ariz. Rev. Stat. Ann. §§ 20-2101 and 2113 (2012)	Disclosure limitations and conditions (Insurance)	Applicable to insurance institutions, insurance producers or insurance support organizations. HMOs are considered "health care services organizations/insurance institutions in the state.
	Ariz. Rev. Stat. Ann. § 36-135 (2012)	Child immunization reporting system; requirements; access; confidentiality; immunity; violation; classification; definitions	Regarding treatment of immunization data.
	Ariz. Rev. Stat. Ann. § 36-509	Confidential records; immunity (mental health)	Restricts disclosure of health information by health care entities (mental health).
	Ariz. Rev. Stat. Ann. § 36-568.01	Confidentiality of records (mental health)	Applies to information obtained in the course of providing services under the "State Department of Developmental Disabilities" chapter (mental health).
	Ariz. Rev. Stat. Ann. § 36-3805	Health Information Organizations — Disclosure of individually identifiable health information	Health information organizations may disclose individually identifiable health information in compliance with HIPAA.
Arkansas			No general/comprehensive prohibition on disclosure of medical information.
	Ark. Code Ann. §§ 14-14-110 and 25-19-105(b)(2)	Personal Information Protection Act; 14-14-110 Public records; 25-19-105 Examination and copying of public records	In general, Arkansas statues prohibit disclosure to the public of any individual's medical information contained in public records.

State	Statue (Citation)	Title of Statute	Comments
	Ark. OHIT Privacy Policy p. 2	Arkansas Office of Health Information Technology (OHIT) Privacy Policies	OHIT policies (applicable to those entities which provide data to State Health Alliance for Records Exchange (SHARE) and "Covered Entities" as defined by HIPAA) are designed to protect personal health information exchange on SHARE.
	Ark. Code Ann. § 23-81-811 (h)	General rules (under Life Settlements Act)	Life insurance licensees entering into life settlement contracts are subject to state medical information confidentiality laws.
	Ark. Code Ann. §23-76-129	Medical information confidential — Exceptions (HMOs)	Generally, HMOs may not disclose any information pertaining to the diagnosis, treatment, or health of any enrollee or applicant obtained from that person or from any provider without the enrollee's or applicant's express consent or under court order.
	54 Ark. Code R. § 74	Insurance Consumer Financial and Health Information Privacy (Insurance)	Restricts insurance company's disclosure of nonpublic personal health information without consumer or customer authorization.
	54 Ark. Code Ann. §20-35-101-103	Genetic Research Nondisclosure Act	Results of genetic research may not be disclosed without the subject's written consent.
California	Cal. Civ. Code § 56.10 (2013)	Authorization for disclosure; When disclosure compelled; When disclosure allowed; Prohibitions	Statute sets out the framework regarding disclosure of medical information absent consent, enumerating specific exceptions when such disclosure may be permitted. California's privacy and security standards extend to businesses organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care upon request, for purposes of managing information, or for diagnosis and treatment.

State	Statue (Citation)	Title of Statute	Comments
	Cal. Health & Safety Code § 121080 (2013)	Consent to disclosure; Form	Confidential research records may be disclosed with prior written consent meeting the criteria established by this rule.
	Cal. Civ. Code § 56.10, § 56.13	56.10 Authorization for disclosure; When disclosure compelled; When disclosure allowed; Prohibitions 56.13 Disclosure by recipient	Redisclosures of medical information are generally prohibited.
	Cal. Ins. Code § 791.13 (2013)	Disclosure of personal or privileged information (Insurance)	Restricts disclosure absent consent by insurance institutions, agents, or insurance-support organizations.
	Cal. Health & Safety Code § 1364.5	Filing of procedures to protect confidentiality; Statement for enrollees and subscribers; Notice of availability (HMOs)	HMOs must file copies of privacy plan to protect patient medical information with the director in order to comply with the Confidentiality of Information Act.
	Cal. Health & Safety Code § 123125 (2013)	Exception for alcohol, drug abuse and communicable disease carrier records	Regarding confidential treatment of alcohol, drug abuse and communicable disease records.
	Cal. Health & Safety Code § 120440 (2013)	Disclosure of Immunization Status	Regarding confidential treatment of immunization records.
	Cal. Wel. & Inst. Code § 5328	The Lanterman-Petris-Short Act	Restricts disclosure of health information by providers (mental health).
	Cal. Health & Safety Code § 103885 (2013)	Cancer Incidence Reporting System; Confidentiality	Regarding confidential treatment of alcohol, drug abuse and immunization records.
	Cal. Ins. Code § 10149.1	Insurance Code (genetic information)	A person may not disclose genetic-related information without written authorization.

State	Statue (Citation)	Title of Statute	Comments
Colorado			No general/comprehensive prohibition on disclosure of medical information.
	Colo. Rev. Stat. § 18-4-412	Theft of medical records or medical information — penalty	Criminal statute (does not apply to covered entities, their business associates, or health oversight agencies as defined under HIPAA). "Medical information" is broadly defined to mean any information contained in the medical record or any information pertaining to the medical, mental health, and health care services performed at the direction of a physician or other licensed health care provider which is protected by the physician-patient privilege established by C.R.S. 13-90-107(1)(d).
	3 Colo. Code Regs. 702-6, R. 6-4-1 Art. 5 § 17	Division of Insurance – Consumer Protection	No authorization is required for any activity that permits disclosure without authorization pursuant to HIPAA. Violations constitute unfair/deceptive trade practice under 3 Colo. Code Regs. 702-6, R. 6-4-1 Art. 6 § 24.
	Colo. Rev. Stat. Ann. § 10-16-423	Confidentiality of health information (HMOs)	HMOs generally may not disclose any information pertaining to the diagnosis, treatment, or health of any enrollee or applicant obtained from that person or from any provider without express consent absent a specifically authorized use.
	Colo. Rev. Stat. Ann. § 25-4-2403	Department of Public Health and Environment — Powers and Duties — Immunization Tracking System — Definitions	Records in the immunization tracking system shall be strictly confidential and shall not be released, shared, or made public, except under defined circumstances.

State	Statue (Citation)	Title of Statute	Comments
	Colo. Rev. Stat. Ann. § 27-10-120 2 Colo. Code Regs. § 502-1, Sctn. 19.360	Care and Treatment of the Mentally Ill	Regarding sharing of mental health treatment information.
	Colo. Rev. Stat. Ann. § 10-3-1104.7	Genetic testing (Regulation of Insurance Companies)	Disclosure of genetic testing information for purposes other than diagnosis, treatment, or therapy requires patient consent. Exemptions include some research uses if the test subject's identity is not released to a third party.
Connecticut			No general/comprehensive prohibition on disclosure of medical information.
	Conn. Gen. Stat. §§ 38a-976; 38a-988	Connecticut Insurance Information and Privacy Protection Act — Definitions; Disclosure limitations and conditions	Restricts disclosure absent consent by insurance institutions, agents and insurance-support organizations. "Medical record information" defined to include personal information which relates to the physical, mental or behavioral health condition, history or treatment, and obtained from a medical professional or medical-care institution, from a pharmacy or pharmacist, from the individual, or from the individual's spouse, parent or legal guardian or from the provision of or payment for health care to or on behalf of an individual or a member of the individual's family. Does not include encrypted or de-identified information.

State	Statue (Citation)	Title of Statute	Comments
	Conn. Gen. Stat. § 38a-988a	Connecticut Insurance Information and Privacy Protection Act — Sale of individually identifiable medical record information	Sale of individually identifiable medical record information prohibited. Written consent re disclosure for marketing purposes. Use of individually identifiable medical record information for clinical research if disclosure otherwise permitted. Applies to health care professional, medical care centers, pharmacies and pharmaceutical companies.
	Conn. Gen. Stat. § 38a-478o	Health Insurance — Confidentiality and antidiscrimination procedures required	Managed care organizations to conform to all applicable state and federal confidentiality statutes.
	Conn. Gen. Stat. § 52-146f	Consent not required for disclosure (mental health)	Regarding sharing of mental health treatment information.
Delaware	Del. Code Tit. 16 § 1212	Disclosure of protected health information	Governs disclosure of protected health information; requires informed consent of the individual except as expressly provided by statute. Statement concerning the DHHS' disclosure policy required upon disclosure.
	Del. Code Tit. 6 § 5002C et. seq.	Safe destruction of records	Statute (effective Jan. 1, 2015) provides that entities seeking to destroy consumer records with personal identifying information, including confidential health care information, must take reasonable steps to make the record undecipherable. An exception applies for health care facilities and insurers who are HIPAA compliant under Del. Code Tit. 6 § 5004C.
	Del. Code. Tit. 18 § 6412	Confidentiality of health information	Applicable to managed care organizations.

State	Statue (Citation)	Title of Statute	Comments
	16 Del. Admin. Code 6001-7.1	Standards Applicable to all Facilities and Programs. 7.1 Clients' Rights	7.1.2.1.9 To confidentiality of all records, correspondence and information relating to assessment, diagnosis and treatment in accordance with 42 U.S.C. § 290dd-2, 42 CFR Part 2 and HIPAA 45 CFR parts 160 and 164.
	16 Del. Admin. Code 6001-8.0	Standards Applicable to all Facilities and Programs. 8.1 Clinical Records	8.1.1.1.4 Comply fully with the provisions of 42 U.S.C. § 290dd-2 and 42 CFR Part 2 and HIPAA 45 CFR parts 160 and 164.
	16 Del. Code §§ 1201-1213	Regulatory Provisions Concerning Public Health — Informed Consent and Confidentiality — Genetic information	Genetic information is confidential, with certain exceptions.
	16 Del. Code § 5161	Mental Health Patients' Bill of Rights — Rights of patients in mental health hospitals or residential centers	Restricts provider disclosure of health information (mental health).
District of Columbia			No general/comprehensive prohibition on disclosure of medical information.
	D.C. Code § 7-242	Use and disclosure of health and human services information	Statute defines when an agency or service provider may use and disclose health care information without consent to another agency or service provider (provided that the use or disclosure is not specifically prohibited under District or federal law). An agency or service provider shall use or disclose individually identifiable health information in accordance with HIPAA.

State	Statue (Citation)	Title of Statute	Comments
	D.C. Code § 31-3426	Confidentiality of medical information and limitation of liability (HMOs)	Health information obtained by any HMO shall be held in confidence and shall not be disclosed absent consent unless an exception is met.
	D.C. Code § 7-3006	Choice in Drug Treatment — Confidential records	All information furnished to APRA [Addiction Prevention and Recovery Administration] pursuant to this chapter shall remain confidential and may be disclosed only to medical personnel for purposes of diagnosis and treatment; except, that with the prior written consent of the client, the information may be disclosed for the purposes of and in accordance with Chapter 2A of this chapter [§ 7-251 et seq.].
	D.C. Code § 31-1606	Prohibition of Discrimination in the Provision of Insurance on Basis of AIDS Test - Informed consent requirements; restrictions on disclosure	Concerning disclosure of AIDS related information.
	D.C. Code § 7-1201.01 et. seq.	Mental Health Information	Concerning disclosure of mental health information.
Florida	Fla. Stat. § 381.026	Florida Patient's Bill of Rights and Responsibilities	Patients have a general right to privacy in health care.
	Fla. Stat. § 456.057	Ownership and control of patient records; report or copies of records to be furnished; disclosure information	Statute governs ownership and control of patient records and disclosure matters.
	Fla. Stat. § 400.611 (nursing home)	Interdisciplinary records of care; confidentiality	Statute governs nursing homes and related health care facilities/interdisciplinary records of care and confidentiality.

State	Statue (Citation)	Title of Statute	Comments
	Fla. Stat. § 395.3025 (hospital licensing and regulation)	Patient and personnel records; copies; examination	Patient records are confidential and must not be disclosed without consent unless a specific exception is met.
	Fla. Stat. § 408.051	Florida Electronic Health Records Exchange Act	Statute details patient authorization of release of electronic health records.
	Fla. Admin. Code Ann. 69J-128.017	Privacy of Consumer Financial and Health Information (Florida Insurance Code) — When authorization required for disclosure of nonpublic personal health information	Statute limits insurers (licensee) disclosure of nonpublic personal health information without consumer or customer authorization.
	Fla. Stat. § 397.501 (2012)	Substance abuse services (7) Right to Confidentiality of Individual Records	Concerning disclosure of substance abuse related information.
	Fla. Stat. § 394.4615 (2012)	Communicable disease and AIDS prevention and control	Access to and limitation of information through state immunization registry.
	Fla. Stat. § 381.004	Public Health — HIV testing	Concerning disclosure of HIV/AIDS related information.
	Fla. Stat. § 394.4615	Clinical records; confidentiality (mental health)	Restricts provider disclosure of medical records (mental health).
Georgia			No general/comprehensive prohibition on disclosure of medical information.
	Ga. Code Ann. § 24-12-11	Disclosure of medical records — Effect on confidential or privileged character thereof	Statute protects redisclosure of medical records, protecting the confidentiality of disclosed confidential or privileged medical matter following any disclosure.

State	Statue (Citation)	Title of Statute	Comments
	Ga. Code Ann. § 33-39-14	Disclosure of personal or privileged information received in connection with insurance transactions (HMOs)	Restricts insurers including HMOs from disclosing personal or privileged information about an individual without written authorization.
	Ga. Code Ann. § 33-21-23	Confidentiality of medical information; claim of privileges by organizations (HMOs)	Any [medical] data obtained by any HMO shall be held in confidence and shall not be disclosed except to the extent that it may be necessary to carry out the purposes of this chapter; or with express consent; or pursuant to statute or court order; or in the event of litigation.
	Ga. Code Ann. §§ 37-7-166	Maintenance, confidentiality, and release of clinical records; disclosure of confidential or privileged patient information (mental health)	Concerning disclosure of records (mental health).
	Ga. Code Ann. § 31-12-3.1	Vaccination registry; reporting requirements, maintenance, and use	Concerning vaccination data reporting requirements.
	Ga. Code Ann.	Treatment of clinical records; when release permitted; scope of privileged communications; liability for disclosure; notice to sheriff of discharge	Restricts provider disclosure of health information (mental health).
	Ga. Code Ann. § 31-7-6	Provision of data for research purposes by organizations rendering patient care; liability of providers of data; use of data; confidentiality	Permitted disclosures (including to approved research groups) for use in study for purpose of reducing rates of morbidity or mortality.
Hawaii	HRS 323B (2012)	Healthcare Privacy Harmonization Act	Prohibits disclosure of confidential medical information. Statute generally provides that compliance with HIPAA constitutes "deemed" compliance with state's existing health care privacy laws.

State	Statue (Citation)	Title of Statute	Comments
	Haw. Rev. Stat. § 432D-21	Confidentiality of medical information (HMOs)	Restricts disclosure of health information by HMOs.
	Haw. Rev. Stat. §§ 325-101	Confidentiality of records and information (HIV/AIDS)	Concerning disclosure of HIV/AIDS-related information.
Idaho			No general/comprehensive prohibition on disclosure of medical information.
	Idaho Code Ann. § 39-3316	Resident rights	Limiting particular groups (i.e., residential care and assisted living facilities) from disclosing information.
	Idaho Code Ann. § 54-1814	Grounds for medical discipline	With respect to physicians, failure to safeguard the confidentiality of medical records or other medical information may be grounds for medical discipline.
	Idaho Code Ann. § 41-3930(1)(d)	Utilization management program requirements	Managed care organizations performing utilization management or contracting with third parties for the performance of utilization management shall…adopt procedures which protect the confidentiality of patient health records.
	Idaho Code Ann. § 66-348	Disclosure of information	Restricts disclosure of records related to an involuntary assessment, detention, or commitment.
	Idaho Code Ann. § 16-2428	Confidentiality and disclosure of information	Restricts disclosure of records related to children's mental health services.
	Idaho Code Ann. § 57-1706 (1995)	Confidentiality	Use of cancer-related information/research.

State	Statue (Citation)	Title of Statute	Comments
	Idaho Admin. Code r. 16.02.10.170	Idaho Reportable Diseases: Cancer	Concerning disclosure of "records", broadly construed to include all communication that identifies any individual who has HIV infection, ARC, or AIDS.
Illinois	410 Ill. Comp. Stat. 50/3 (2012)	Patients' rights	Statute provides for a right of each patient to privacy and confidentiality in health care.
	215 Ill. Comp. Stat. 5/1014 (2012)	Disclosure Limitations and Conditions (Insurance Information and Privacy Protection)	Statute limits disclosure of personal or privileged information by insurance institutions, agents or insurance-support organizations without consent, unless an exception is met. Note that Illinois Insurance Information and Privacy Protection Act applies to HMOs as well as insurance entities.
	20 Ill. Comp. Stat. 301/30-5 (2012)	Alcoholism and Other Drug Abuse and Dependency Act — Patients' Rights	Concerns records of the identity, diagnosis, prognosis or treatment of any patient maintained in connection with the performance of any program or activity relating to alcohol or other drug abuse or dependency education; early intervention; intervention; training; treatment or rehabilitation regulated, authorized, or directly or indirectly assisted by any Department or agency.
	410 Ill. Comp. Stat. 527/10, 527/20 (2012)	Immunization Data Registry Act	527/20: Confidentiality of information; release of information; statistics; panel on expanding access. (a) Records maintained as part of the immunization data registry are confidential.
	740 Ill. Comp. Stat. §§ 110/3-110/7, 110/9.1-9.4	Mental Health and Developmental Disabilities Confidentiality Act	Restricts provider disclosure of records (mental health).

State	Statue (Citation)	Title of Statute	Comments
Indiana			No general/comprehensive prohibition on disclosure of medical information.
	Ind. Code § 16-39-1-4	Contents of written consent for release	Statute describes requirements for release of patient's health record.
	Ind. Code §16-40-4-7	Confidentiality of information from which identity may be ascertained	Statute governs the confidentiality of health care quality indicator data and other information collected under this chapter, or resulting from 2006 state program to collect health care quality indicator data for individuals who reside/receive care in Indiana.
	Ind. Code § 16-39-5-3	Provider's use of records; confidentiality; violations	Use of original health record for legitimate business purposes.
	Ind. Code § 27-8-26	Genetic screening or testing	Statute limits access and use by insurance companies to genetic data.
	Ind. Code § 27-13-31-1	Confidential information (HMOs)	Provides that any information that pertains to the diagnosis, treatment, or health of any enrollee of an HMO or limited service HMO is confidential and may not be disclosed without consent.
	Ind. Code § 16-38-4-12	Release of confidential information	Applicable to researchers.
	Ind. Code §§ 16-39-2-2 – 16-39-2-12	Release of Mental Health Records to Patient and Authorized Persons	Restricts provider disclosure of records (mental health).
	Ind. Code § 16-38-2-5 et. seq.	Cancer Registry; Access to Confidential Information for Research Purposes	Access to confidential information for research purposes; release of confidential information by state department.

State	Statue (Citation)	Title of Statute	Comments
Iowa	Iowa Code Ann. § 22.7(2) (2014)	Confidential records	Hospital records, medical records, and professional counselor records of the condition, diagnosis, care, or treatment of a patient or former patient or a counselee or former counselee, including outpatient are "confidential unless otherwise ordered…by another person duly authorized to release such information."
	Iowa Admin. Code r. 191-90.1 et. seq. (505)(2014)	Insurance Division — Financial and Health Information Regulation	Governs the treatment of nonpublic personal financial information and nonpublic personal health information about individuals by all licensees of the insurance division. Exceptions apply for, among other things, actuarial, scientific, medical or public policy research; any activity that permits disclosure without authorization pursuant to HIPAA; and any activity otherwise permitted or required by law. Compliance with HIPAA shall be deemed compliance with the Iowa requirements. (Iowa Admin. Code r. 191-90.20(505)(2014)).
	Iowa Admin. Code r. 191-90.17	Insurance Division — Financial and Health Information Regulation — Disclosure of nonpublic personal health information	Statute provides that a licensee shall not disclose nonpublic personal health information without authorization unless an exception applies.
	Iowa Code Ann. § 514B.30 (1992)	Communications in professional confidence (HMOs)	Restricts disclosure of privileged communications by health maintenance organizations.
	Iowa Admin. Code r. 441-88.9(249A)(2013)	Managed Health Care Providers — Records and reports	HMOs must maintain the confidentiality of medical record information and release the information only with consent unless a specific exception is met.
	Iowa Code Ann. § 228.2	Mental Health Information Disclosure Prohibited — exceptions — Record of disclosure	Restricts provider disclosure of information (mental health).

State	Statue (Citation)	Title of Statute	Comments
	Iowa Code Ann. § 141A.9	Acquired Immune Deficiency Syndrome (AIDS) — Confidentiality of information	Concerning disclosure of HIV/AIDS-related information.
Kansas			No general/comprehensive provisions governing confidentiality of health care data.
	Kan. Stat. Ann. § 65-1525	Confidentiality of communications	Specific confidentiality provisions apply to categories of licensed professionals.
	Kan. Stat. Ann. 65-6821 through 65-6834 and 65-6835	Kansas Health Information Technology Act	Statute designed to harmonize state law with the HIPAA privacy rule.
	Kan. Stat. Ann. 65-6825	Same; use and disclosure of protected health information	Statute provides that no covered entity shall use or disclose health information without consent unless specific exceptions are met, including to an HIO (requirements apply).
	Kan. Stat. Ann. § 40-3226	Confidentiality of medical information (HMOs)	Statute provides for general confidentiality of health information obtained by HMOs.
	Kan. Admin. Regs. 40-1-46	Insurance Department — Privacy of consumer financial and health information	Adopts by reference the National Association of Insurance Commissioners' "privacy of consumer financial and health information regulation", with exception.
	Kan. Stat. Ann. § 65-5602	Privilege of patient of treatment facility to prevent disclosure of treatment and of confidential communications; extent of privilege; persons who may claim privilege; persons to which confidential communications extend	Concerning confidential communications made for the purposes of diagnosis or treatment of the patient's mental, alcoholic, drug dependency or emotional condition.

State	Statue (Citation)	Title of Statute	Comments
	Kan. Stat. Ann. § 65-6002	Public Health — Acquired Immune Deficiency Syndrome (AIDS) and Hepatitis B; Other infectious disease	Concerning disclosure of HIV/AIDS-related information.
	Kan. Stat. Ann. § 65-531(c) (2010)	Immunization information and records; disclosure	Information and records which pertain to the immunization status of persons against childhood diseases as required by K.S.A. 65-508, and amendments thereto, whose parent or guardian has submitted a written statement of religious objection to immunization as provided in K.S.A. 65-508, and amendments thereto, may not be disclosed or exchanged without a parent or guardian's written release authorizing such disclosure.
Kentucky			No general/comprehensive prohibition on disclosure of medical information.
	902 Ky. Admin. Regs. 20:054	Health maintenance organizations; operations and services	A health maintenance organization shall have written policies that assure confidential treatment of enrollee records and disclosures, and afforded enrollees the opportunity to approve or refuse their release to any individual not involved in his care except as required by law or third-party payment contract.
	Ky. Rev. Stat. Ann. § 222.271(1) (2014)	Confidential record of treatment — Rights of patient	The administrator of each program shall keep a record of the treatment afforded each alcohol and other drug abuse patient, which shall be confidential in accordance with administrative regulations promulgated by the cabinet.

State	Statue (Citation)	Title of Statute	Comments
	Ky. Rev. Stat. Ann. § 211.670(1) (2014)	Confidentiality of registry reports and records — Use of information	All lists and medical records maintained by hospitals and medical laboratories pursuant to KRS 211.660 shall be confidential. All information collected and analyzed pursuant to KRS 211.660 and 211.665 shall be held confidential as to the identity of the individual patient.
	Ky. Rev. Stat. Ann. § 304.17A-846(2) (2014)	Providing of requested information on insureds by group health benefit plan insurers — Confidentiality — Additional information to be provided to large groups	Statute regarding insurer disclosure of nonpublic personal health information without the written consent of the individual who is the subject of the information, as required by administrative regulations promulgated by the commissioner.
	Ky. Rev. Stat. Ann. § 210.235	Confidential nature of records (mental health)	Restricts provider disclosure of health information (mental health).
	Ky. Rev. Stat. Ann. § 214.556	Kentucky Cancer Registry — Cancer patient data management system	Specific disclosure rules apply to reporting of cancer cases.
	Ky. Rev. Stat. Ann. § 214.645	Reporting system of HIV-positive persons — Confidentiality and reporting requirements	Concerning disclosure of HIV/AIDS-related information.
Louisiana			No general/comprehensive prohibition on disclosure of medical information.
	La. Rev. Stat. Ann. § 22:1023.7(C)	Prohibited discrimination; genetic information; disclosure requirements; definitions (Insurance)	Statute limits access and use by insurance companies to genetic data.
	La. Rev. Stat. Ann. § 22:265	Confidentiality of medical information (HMOs)	Provides that any information that pertains to the diagnosis, treatment, or health of any enrollee of an HMO is confidential and may not be disclosed without consent.

State	Statue (Citation)	Title of Statute	Comments
Maine	Me. Rev. Stat. Ann. Tit. 22 § 1711-C	Health and Welfare- Hospitals and Medical Care — Confidentiality of health care information Patient access to hospital medical records	An individual's health care information is confidential and may not be disclosed other than to the individual by the health care practitioner or facility unless an exception applies.
	Me. Rev. Stat. Ann. 24-A § 2215	Disclosure limitations and conditions	Statute governs disclosure by regulated insurance entity or insurance support organization of personal information about a consumer collected or received in connection with an insurance transaction.
	Me. Rev. Stat. Ann. 24-A § 4224	Confidentiality; liability; access to records (HMOs)	Restricts disclosure of personal information by health maintenance organizations.
	Me. Rev. Stat. Ann. 5, § 20047 (2012)	Records	Registration and other records of treatment facilities (alcoholism and drug abuse).
	10-144-280 Me. Code R. § 7	Confidentiality of All Reporting Data	All data reported to the Maine Birth Defects Program, which contains either direct or indirect individually identifiable information, shall be confidential.
	Me. Rev. Stat. Ann. 34-B § 1207	Confidentiality of Information (mental health)	Restricts provider disclosure of health information (mental health).
	Me. Rev. Stat. Ann. 5 § 19203	Public Health — Medical conditions — Confidentiality of test	Concerning disclosure of HIV/AIDS-related information.
Maryland	Md. Code Ann. Health-Gen. § 4-302	Confidentiality and disclosure generally	Statute governs confidentiality of medical records. Among other things, it specifically provides that a person may not disclose any medical record by sale, rental, or barter.

State	Statue (Citation)	Title of Statute	Comments
	Md. Code Ann. Health-Gen. § 4-301	Definitions	"Medical record" defined as any information in any form entered in the record that identifies or can readily be associated with the identity of a patient or recipient, and that relates to the health care of the patient or recipient.
	Md. Code Ann. Ins. § 4-403	Disclosure of insured's medical or claim records	An insurer, or an insurance service organization whose functions include the collection of medical data, may not disclose the contents of an insured's medical or claims records, except [among other permitted exceptions] if the use does not disclose the identity of a particular insured or covered person. All disclosures subject to HIPAA.
	Md. Code Ann. Health-Gen. § 8-601	Privileged Information Concerning Individual Treatment in Counseling for Drug, Alcohol Abuse	Disclosure and use of records (alcohol abuse and drug abuse treatment programs).
	Md. Code Regs. §4-307	Mental Health Record Disclosures	Restricts provider disclosure of health information (mental health).
	Md. Code Ann. Health-Gen. § 18-204 Md. Code Regs. § 10.14.01.07	Confidentiality of Cancer Reports	Concerning disclosure of cancer data.
	Md. Human Services Code Ann. §9-219	Human Services — Confidential research record	Concerns confidentiality of research studies.

State	Statue (Citation)	Title of Statute	Comments
Massachusetts	M.G.L. 111 § 70E	Patients' Rights — Health Care Facilities	Massachusetts has a patient bill of rights, under which every patient or resident of a hospital or other facility shall have the right [among other things]... to confidentiality of all records and communications to the extent provided by law. A violation of rights under this section may be subject to a civil action. In addition, Massachusetts has statutes governing specific entities and medical conditions. Hospital and other facilities' records are confidential to the extent provided by law, with certain exceptions.
	M.G.L. 214 § 1B	Right of Privacy; Remedy to Enforce	A person shall have a right against unreasonable, substantial or serious interference with his privacy.
	M.G.L. 175I § 13	Disclosure of Personal or Privileged Information to Third Parties; Restrictions (Insurance)	Statute restricts disclosure by insurance institutions, insurance representatives or insurance-support organizations.
	M.G.L. 176G § 4B	Disclosure of Information — Mental Health	Restricts provider disclosure of health information (mental health).
	105 Mass. Code Regs. 164.084	Confidentiality	Client-specific information shall be privileged and confidential and shall be made available only in conformity with all applicable state and federal laws and regulations regarding the confidentiality of client records, including but not limited to HIPAA Privacy and Security Rules, if applicable.
	105 Mass. Code Regs. 302.070	Confidentiality	Regarding information collected by the Congenital Anomalies Registry.
	M.G.L. 112 § 129A	Confidential Communications	Restricts provider disclosure of health information (mental health).

State	Statue (Citation)	Title of Statute	Comments
	M.G.L. 233 § 20B	Privileged Communications; patients and psychotherapists; exceptions	Applies specific restrictions to health maintenance organizations.
	M.G.L. 111 § 70F	Public Health — HIV test; informed consent; disclosure of results or identity of subject of test.	Concerning disclosure of HIV/AIDS-related information.
	M.G.L. 111 § 70G	Public Health — Genetic information and reports protected as private information	Confidential treatment of any written or recorded individually identifiable result of a genetic test as defined by this section or explanation of such a result.
	105 Mass. Code Regs. 301.040	Cancer Registry; Confidentiality of Reports	Concerning disclosure of cancer data.
Michigan			No general/comprehensive prohibition on disclosure of medical information.
	Mich. Comp. Laws § 333.20201	Policy describing rights and responsibilities of patients or residents; adoption; posting and distribution; contents; additional requirements; discharging, harassing, retaliating, or discriminating against patient exercising protected right; exercise of rights by patient's representative; informing patient or resident of policy; designation of person to exercise rights and responsibilities; additional patients' rights; definitions	A health facility or agency that provides services directly to patients or residents shall adopt a policy that among other things covers confidential treatment of personal and medical records.

State	Statue (Citation)	Title of Statute	Comments
	Mich. Comp. Laws § 333.17752 (pharmacists)	Prescription or equivalent record; preservation; disclosure; providing copies; refilling copy; applicability of subsection (3) to pharmacies sharing real-time, on-line database	Disclosure of prescriptions prohibited without patient's consent.
	Mich Comp. Laws § 331.531	Act 270 of 1967 Release of Information for Medical Research and Education	Allows release of health information and data to review entities.
	Mich. Admin. Code r. 325.6810	Clinical patient records; confidentiality; disclosure; availability; storage and preservation	"Information contained in the clinical patient record shall be treated as confidential, shall be disclosed only to authorized persons, and shall be available at all times to the [Department of Community Health] for purposes of examination and review."
	Mich. Comp. Laws § 333.5131	Public Health Code — Serious communicable diseases or infections of HIV infection and acquired immunodeficiency syndrome; confidentiality of reports	Concerning disclosure of HIV/AIDS-related information.
	Mich. Comp. Laws § 333.6111 et. seq.	Public Health Code — Records confidential, limitations on disclosure	Concerning confidentiality of records in connection with the performance of a licensed substance abuse treatment and rehabilitation service, a licensed prevention service, an approved service program, or an emergency medical service authorized or provided or assisted under this article.
	Mich. Comp. Laws § 333.17020	Public Health Code — Genetic test (consent)	Concerning disclosure of genetic information.
	Mich. Comp. Laws § 330.1748	Confidentiality (insurance)	Restricts insurer disclosure of health information (mental health).

State	Statue (Citation)	Title of Statute	Comments
Minnesota	Minn. Stat. § 144.293	Release or Disclosure of Health Records	Statute governs the release and disclosure of records generally.
	Minn. Stat. § 144.651	Health Care Bill of Rights	Section 16 governs confidentiality of personal and medical records.
	Minn. Stat. § 144.053	Research Studies Confidential	Statute requires state health commissioner to keep all state health research data confidential.
	Minn. Stat. § 72A.502	Disclosure of Information; Limitations and Conditions (Insurance)	Statute restricts disclosure by insurers, insurance agents, or insurance-support organizations.
	Minn. Stat. § 72A.139	Genetic Discrimination Act	Concerning disclosure of genetic information.
	Minn. Stat. § 62D.145	Disclosure of information held by health maintenance organizations	Statute covers disclosure of information held by HMOs.
	Minn. Stat. § 254A.09 (2012)	Confidentiality of Records	The Department of Human Services shall assure confidentiality to individuals who are the subject of research by the state authority or are recipients of alcohol or drug abuse information, assessment, or treatment from a licensed or approved program.
	Minn. Stat. § 144.671 et. seq.	Cancer Surveillance System	Cancer reporting requirements.
	Minn. Stat. § 144.3351 (2012)	Immunization Data	Regarding immunization information.
	Minn. Stat. § 144.2219 (2012)	Transfers of Information to Research Entities	Regarding birth defects information.

State	Statue (Citation)	Title of Statute	Comments
	Minn. Stat. § 144.294	Records Relating to Mental Health	Restricts provider disclosure of health information (mental health).
Mississippi			No general/comprehensive prohibition on disclosure of medical information.
	Miss. Code Ann. § 41-9-67	Hospital records not public records; privileged communications rule not impaired	Statute maintains that hospital records are not public records.
	Miss. Code Ann. § 83-41-355	Confidentiality of data or information; claims of privilege; civil liability of members of health review committees; discovery of information considered by and records of health review committees; access to treatment records, etc., of enrollees	Statute provides that any information that pertains to the diagnosis, treatment, or health of any enrollee or applicant of an HMO may not be disclosed without express consent.
	Miss. Code Ann. § 41-21-97	Public Health — Individuals with mental illness or an intellectual disability — Confidentiality of hospital records and information; exceptions	Restricts provider disclosure of health information (mental health).
Missouri			No general/comprehensive prohibition on disclosure of medical information.
	13 CSR 70-1.020	Standards for Privacy of Individually Identifiable Health Information	Statute required the entire health care industry to implement HIPAA, including state governments.

State	Statue (Citation)	Title of Statute	Comments
	20 CSR 2220-2.300	Record Confidentiality and Disclosure (pharmacy only)	Statute establishes requirements for the confidentiality and disclosure of records related to patient care. Confidential records shall not be released to anyone except the patient, a provider… [or] a person or entity to whom such information may be disclosed under HIPAA.
	Mo. Rev. Stat.§ 192.067	Patients' medical records, department may receive information from — purpose — confidentiality — immunity for persons releasing records, exception — penalty — costs, how paid	Statute allows patient information to be collected and analyzed by the department of health and senior services for epidemiological studies.
	Mo. Rev. Stat.§ 192.650	Public Health and Welfare — Cancer information reporting system established — purpose-rulemaking authority	Governs cancer information reporting system.
	Mo. Rev. Stat.§ 354.515	Confidential information, diagnosis, treatment, health of enrollees or applicants, exceptions	Statute prohibits HMOs from disclosing health, diagnosis, or treatment information of an enrollee without express consent.
	Mo. Rev. Stat. § 167.183	Immunization records, disclosure, to whom — disclosure for unauthorized purpose, liability	Concerns disclosure of immunization records.
	Mo. Rev. Stat. 354.515	Confidential information, diagnosis, treatment, health of enrollees or applicants, exceptions — confidentiality of mental health records	Restricts provider and HMO disclosure of health information (mental health).
Montana	Mont. Code Ann. § 50-16-501 to 553	Uniform Health Care Information Act	Prohibits health care providers from disclosing health care information about a patient without written consent.

State	Statue (Citation)	Title of Statute	Comments
	Mont. Code Ann. § 33-19-306(1)	Disclosure limitations and conditions	Montana's Insurance Information and Privacy Protection Act prohibits a licensee from disclosing personal or privileged information collected or received in connection with an insurance transaction. HMOs are also subject to Montana's Insurance Information and Privacy Protection Act.
	Mont Code Ann. § 33-19-307(2)	Personal information used for marketing purposes — restrictions	A licensee may not use or disclose medical record information for marketing purposes.
	Mont. Code Ann. § 33-31-113	Confidentiality of medical information	Statute provides that any information that pertains to the diagnosis, treatment, or health of any enrollee or applicant of an HMO are confidential and may not be disclosed without consent.
Nebraska			No general/comprehensive prohibition on disclosure of medical information.
	Neb. Rev. Stat. § 38-1225	Patient data; confidentiality; immunity	Statute prohibits emergency medical services and out-of hospital emergency care providers from releasing patient data it has received or recorded with certain treatment, payment and health care operation exceptions defined in HIPAA.
	Neb. Rev. Stat. § 44-901, *et seq*.	Privacy of Insurance Consumer Information Act	Statute limits licensed insurers ability to disclose nonpublic personal health information without authorization and requires notice to individuals of licensee's policies and practice unless the licensee complies with HIPAA.

State	Statue (Citation)	Title of Statute	Comments
	Neb. Rev. Stat. § 44-32,172	Confidential information; disclosure prohibited; exception	Statute provides that any information that pertains to the diagnosis, treatment, or health of any enrollee or applicant of an HMO are confidential and may not be disclosed without consent or as necessary to carry out the purposes of the HMO Act.
Nevada			No general/comprehensive prohibition on disclosure of medical information.
	Nev. Rev. Stat. § 439.590	Requirements for participation in system; limitations on use, release or publication of certain information; penalty for unauthorized access to electronic health record, system or health information exchange; establishment of complaint system	Statute establishes a statewide health information exchange system that restricts use of electronic health record information for marketing purposes or use unrelated to treatment, care, well-being or billing.
	Nev. Rev. Stat. § 439.538	Electronic transmission of health information: Exemption from state law concerning privacy or confidentiality of certain health information; ability of person to opt out of electronic disclosure of certain health information	Statute exempts covered entities that transmit electronic data in compliance with HIPAA from more stringent state laws regarding privacy and confidentiality.
	Nev. Rev. Stat. § 695F.410	Confidentiality and disclosure of information	Statute prohibits prepaid limited health service organization from disclosing any information related to diagnosis, treatment, or health of any enrollee or applicant unless written consent is provided.
	Nev. Rev. Stat. § 433A.360	Clinical records: contents; confidentiality (mental health)	Restricts provider disclosure of health information (mental health).

State	Statue (Citation)	Title of Statute	Comments
New Hampshire	N.H. Rev. Stat. Ann. § 151:21	Patients' Bill of Rights	Patients' bill of rights, providing that the patient shall be ensured confidential treatment of all information contained in the patient's personal and clinical record, including that stored in an automatic data bank, and the patient's written consent shall be required for the release of information to anyone not otherwise authorized by law to receive it.
	N.H. Rev. Stat. Ann. § 332-I:1	Medical Records; Definitions	Release or use of patient identifiable medical information for the purpose of sales or marketing of services or products prohibited without written authorization.
	N.H. Rev. Stat. Ann. § 318:47-f	Prescription Information to be Kept Confidential	Concerns treatment of prescription information containing patient-identifiable and prescriber-identifiable data for any commercial purpose.
	N.H. Rev. Stat. Ann. § 332-I:3	Use and Disclosure of Protected Health Information; Health Information Exchange	Establishing framework for providers and their business associates to transmit protected health information through the health information organization ("HIO").
	N.H. Rev. Stat. Ann. § 332-I:5	Unauthorized Disclosure	Statute provides that if there is a use or disclosure of protected health information allowed under federal law but not permitted by RSA 332-I:4, the health care provider shall promptly notify in writing the individual or individuals whose protected health information was disclosed.
	N.H. Rev. Stat. Ann. § 420-J:10	Confidentiality of Insurer Records	Confidentiality of insurer records, specifically data or information pertaining to the diagnosis, treatment, or health of a covered person.

State	Statue (Citation)	Title of Statute	Comments
	N.H. Code R. Ins. 3005.01	When Authorization Required for Disclosure of Nonpublic Personal Health Information	A licensee shall not disclose nonpublic personal health information about a consumer or customer without authorization, unless a specific exception is met, including any activity that permits disclosure without authorization pursuant to HIPAA.
	N.H. Code R. Ins. 3005.05	3005.04 Relationship to Federal Rules 3005.05 Relationship to State Laws	Irrespective of whether a licensee is subject to HIPAA, under N.H. Code R. Ins. 3005.04, if a licensee complies with all requirements of such rule except for its effective date provision, the licensee shall not be subject to the provisions of this section. The Insurance Code does not preempt or supersede existing state law related to medical records, health or insurance information privacy under N.H. Code R. Ins. 3005.05.
	N.H. Rev. Stat. Ann. § 172:8-a	Confidentiality of Client Records	Confidentiality of records (alcohol or drug abuse treatment).
	N.H. Rev. Stat. Ann. § 330-C:26	Privileged Communications Between Licensees and Certificate Holders and Their Clients	Regarding information collected in connection with substance use counseling services.
	N.H. Rev. Stat. Ann. § 135-C:19-a	Disclosure of Certain Information (mental health)	Concerning disclosure of medical records (mental health).
New Jersey			No general/comprehensive prohibition on disclosure of medical information.

State	Statue (Citation)	Title of Statute	Comments
	N.J. Stat. Ann. § 26:2H-12.8	Rights of persons admitted to a general hospital	Patient right to privacy and confidentiality of all records pertaining to the patient's treatment, except as otherwise provided by law or third party payment contract, and to access those records.
	N.J. Stat. Ann. § 17:23A-13	Disclosure limitations and conditions (Insurance)	Statute enumerates disclosure limitations and conditions applicable to insurance institutions, agents and insurance-support organizations.
	N.J.A.C. § 11:22-4.13	Confidentiality (Insurance)	Any data or information relating to the diagnosis, treatment or health of an enrollee, prospective enrollee or contract holder obtained by a licensed organized delivery system from the carrier, contract holder, enrollee, prospective enrollee or any provider shall be confidential and shall not be disclosed to any person except as provided by N.J.S.A. 17:48H-30.
	N.J. Stat. Ann. § 26:2J-27	Confidentiality of medical information (HMOs)	Statute restricts disclosure of any data or information pertaining to the diagnosis, treatment, or health of any enrollee or applicant obtained from such enrollee or from any provider by any health maintenance organization.
	N.J. Stat. Ann. § 26:4-138(8)	Certain transmissions of information permitted	Regarding transmission or exchange of immunization information.
	N.J. Stat. Ann. § 30:4-24.3; N.J.A.C. § 10:37-6.79	Confidentiality; exceptions	Restricts provider disclosure of health information (mental health).
	N.J. Stat. Ann. § 10:5-47	Civil Rights — Conditions for disclosure of genetic information	Concerning disclosure of genetic information.

State	Statue (Citation)	Title of Statute	Comments
New Mexico			No general/comprehensive prohibition on disclosure of medical information.
	N.M. Code R. § 8.300.11.9	Confidentiality	Medical services, medical data including diagnosis and past history of disease or disability, and other identifying data is confidential and is safeguarded by the human services department (HSD), all state agencies, their contractors and other authorized agents and all providers of Medical Assistance Division ("MAD") services.
	N.M. Stat. Ann. § 14-6-1	Health information; confidentiality; immunity from liability for furnishing	Statute provides that all health information that relates to and identifies specific individuals as patients is strictly confidential and shall not be a matter of public record or accessible to the public.
	N.M. Stat. Ann. § 24-14B-6	Health information system; creation; access	Governs treatment/access to information submitted to HIO.
	N.M. Stat. Ann. § 24-14B-6	Use and disclosure of electronic health care information	Statute further provides that a provider, health care institution, health information exchange or health care group purchaser shall not use or disclose health care information in an individual's electronic medical record to another person without the consent of the individual except as allowed by state or federal law.

State	Statue (Citation)	Title of Statute	Comments
	N.M. Code R § 13.1.3.1 *et. seq*.	Privacy of nonpublic personal information (Insurance)	There are also provisions related to confidentiality of health and financial records in N.M. Code R § 13.1.3 *et. seq*. "Nonpublic personal health information" is defined in N.M. Code R. § 13.1.3.7 to mean "health information (1) that identifies an individual who is the subject of the information; or (2) with respect to which there is a reasonable basis to believe that the information could be used to identify an individual." N.M. Code R. § 13.1.3.14 sets out the limits on disclosure of nonpublic personal information; and N.M. Code R. § 13.3.15 governs redisclosure.
	N.M. Code R. § 8.300.11.11	Confidentiality of electronic data	Regulation governing the confidentiality of electronic data.
	N.M. Stat. Ann § 24-1-20	Records confidential	Statute governs information related to public health research.
	N.M. Stat. Ann. § 59A-46-27	Confidentiality of medical information and limitation of liability	Statute governs confidentiality of medical information obtained by any health maintenance organization.
	N.M. Stat. Ann. § 7.1.3.19	Exempted Records	All records of the department are public records unless the record is exempted under state or federal law or regulation. Exemptions apply for records under the Drug Abuse Treatment Act, Section 26-2-12 and 14 NMSA 1978; Confidentiality of Alcohol and Drug Abuse Patient Records, 42 U.S.C. Section 290dd-2 and 290ee-3; and 42 CFR 2.1 to 2.67.
New York			No general/comprehensive prohibition on disclosure of medical information.

State	Statue (Citation)	Title of Statute	Comments
	N.Y. Pub. Health Law § 18 (6)	Access to patient information	Statute requires a copy of the subject's written authorization and purpose of disclosure whenever a health care provider, as otherwise authorized by law, discloses patient information to a third party.
	N.Y. Comp. Codes R. & R. tit. 11 § 420.17	When authorization required for disclosure of nonpublic personal health information (Insurance)	Statute states licensee may not disclose nonpublic personal information without consumer or customer authorization.
	N.Y. Pub. Health Law § 18(1)(c)	Access to patient information	N.Y. Pub. Health Law § 18 includes HMOs in the definition of "health care facility" restricting disclosure to third parties without written authorization.
	N.Y. Pub. Health Law §4410	Health maintenance organizations; professional services	HMOs may not disclose any information which was acquired in the course of rendering to a patient of professional services by an authorized practitioner unless the patient waives the right of confidentiality.
	NY Pub. Health § 2168 (2012)	Statewide immunization information system	A person, institution or agency to whom immunization information is given, shall not divulge any part thereof so as to disclose the identity of such person to whom such information or record relates, except insofar as such disclosure is necessary for the best interests of the person or other persons, consistent with the purposes of this section.
	NY Men. Hyg. § 33.13	Clinical records; confidentiality	Restricts provider disclosure of health information (mental health).
	N.Y. Pub. Health Law § 2782	Public Health — HIV related testing — Confidentiality and disclosure	Concerning disclosure of HIV/AIDS-related information.

State	Statue (Citation)	Title of Statute	Comments
North Carolina			No general/comprehensive prohibition on disclosure of medical information.
	N.C. Gen. Stat. § 90-21.20B	Access to and disclosure of medical information for certain purposes	A health care provider may disclose protected health information for purposes of treatment, payment, or health care operations (as defined in HIPAA) to the extent that disclosure is permitted under 45 C.F.R. §164.506 and is not specifically prohibited by other state or federal law.
	N.C. Gen. Stat. § 90-412	Electronic medical records	Statute extends legal rights and responsibilities of patients, health care providers, facilities, and governmental units to electronic records.
	10A N.C. Admin. Code 69 .0301	Right of Access	Confidentiality of information about himself is the right of the client [applicant or recipient of public assistance or services – from Division of Social Services].
	10A N.C. Admin. Code 69 .0502 - 0503	Disclosure for the purpose of research	Regarding disclosure of client [of Department of Social Services] information.
	N.C. Gen Stat. § 58-39-75	Disclosure limitations and conditions (Insurance)	Restricts disclosure of personal or privileged information by any insurance institution, agent, or insurance-support organization.
	N.C. Gen. Stat. § 90-412	Electronic medical records	"The legal rights and responsibilities of patients, health care providers, facilities, and governmental units shall apply to records created or maintained in electronic form to the same extent as those rights and responsibilities apply to medical records embodied in paper or other media. This subsection applies with respect to the security, confidentiality, accuracy, integrity, access to, and disclosure of medical records."

State	Statue (Citation)	Title of Statute	Comments
	N.C. Gen. Stat. § 58-67-180	Confidentiality of medical information (HMOs)	Health data obtained by any HMO shall be held in confidence and shall not be disclosed except as set forth.
	N.C. Gen. Stat. §§ 122C-52 – 122C-56; 10A N.C. Admin. Code §§ 26B.0101, 0201, 0206, 0207, 0209	Right to confidentiality	Restricts provider disclosure of health information (mental health).
	10 A N.C. Admin. Code § 47B.0106	Release of Central Cancer Registry Data For Research	Concerning cancer information reporting.
North Dakota			No general/comprehensive prohibition on disclosure of medical information.
	N.D. Cent. Code § 26.1-36-12.4	Confidentiality of medical information (Insurance)	Statute prohibits insurer from disclosing any identifiable data or information relating to diagnosis, treatment or health of any enrollee or applicant without written, dated consent.
	N.D. Cent. Code §§ 26.1-36-03.1	Information disclosure; Confidentiality of medical information	Insurance companies and HMOs may not deliver, execute, issue or renew health insurance policy unless confidentiality of information is ensured.
	N.D. Admin. Code 45-14-01-17	When authorization required for disclosure of nonpublic personal health information (Insurance)	Licensees may not disclose nonpublic personal health information without consumer or customer authorization.

State	Statue (Citation)	Title of Statute	Comments
	N.D. Cent. Code § 26.1-18.1-23	Confidentiality of medical information and liability (HMOs)	Statute provides that any information that pertains to the diagnosis, treatment, or health of any enrollee or applicant of an HMO are confidential and may not be disclosed without consent.
Ohio	Ohio Rev. Code Ann. § 3798 et. seq.	Health-Safety-Morals — Protected Health Information	Statute requires compliance by a covered entity with HIPAA in connection with the use or disclose protected health information. The stated intent of the legislature was to be consistent with HIPAA for the purpose of eliminating barriers to the adoption and use of electronic health records and health information exchanges. (Ohio Rev. Code Ann. § 3798.02)
	Ohio Rev. Code § 3904.13	When personal or privileged information may be disclosed	Insurers may not disclose personal or privileged information collected in connection with an insurance transaction without written authorization.
	Ohio Rev. Code § 3701.243	Disclosing of HIV test results or diagnosis	Regarding confidentiality of HIV/AIDS information.
	Ohio Rev. Code § 122.31	Public Welfare — Hospitalization of mentally ill	Regarding confidentiality of health information (mental health).
	Oh. Rev. Code §3701.263	Confidentiality	Regarding disclosure of cancer information.
Oklahoma			No general/comprehensive prohibition on disclosure of medical information.

State	Statue (Citation)	Title of Statute	Comments
	Okla. Admin. Code § 365:35-1-40	When authorization required for disclosure of nonpublic personal health information (Insurance)	Under the Privacy of Consumer Financial and Health Information Regulation a licensee may not disclose nonpublic personal health information about an insurance consumer or customer without authorization.
	Okla. Admin. Code § 365:35-1-43	Relationship to federal rules (Insurance)	Insurers who comply with HIPAA do not need to meet state regulations.
	Okla. Stat. Tit. 36 § 6927	Public records — Trade secrets — Privileged or confidential information (HMOs)	Statute describes what information obtained by HMOs is privileged or confidential.
Oregon	Or. Rev. Stat. § 192.502(2)	Other public records exempt from disclosure	Exempts medical information from public disclosure unless there is clear and convincing evidence of public interest that would require disclosure.
	Or. Rev. Stat. § 192.556(1) & (6)	Definitions	Individual has the right to have protected health information safeguarded from unlawful use or disclosure.
	Or. Rev. Stat. § 192.558	Health care provider and state health plan authority	Statute allows a health care provider or state health plan to disclose personal health information in a manner consistent with the individual's authorization.
	Or. Rev. Stat. § 746.665(1)	Limitations and conditions on disclosure of certain information (Insurance)	Statute restricts an insurer's ability to disclose medical information about an individual collected or received in connection with an insurance transaction without person's written authorization.
	Or. Rev. Stat. § 746.665(k)	Limitations and conditions on disclosure of certain information (Insurance)	Statute prohibits insurance entities from disclosing medical record information for marketing purposes without prior written consent.

State	Statue (Citation)	Title of Statute	Comments
	Or. Rev. Stat § 413.301 to 308	Health Information Technology Oversight Council	Statute establishes Health Information Technology Oversight Council to monitor health information technology privacy and security.
	Or. Rev. Stat § 432.530	Confidentiality of information (cancer)	Identifying information reported under Or. Rev. Stat §432.520 (cancer reporting requirement) shall be confidential and privileged.
	Or. Rev. Stat § 433.045	Consent to HIV test required; exceptions	Regarding confidentiality of HIV/AIDS information.
Pennsylvania			No general/comprehensive prohibition on disclosure of medical information.
	31 Pa. Cons. Stat § 146b.11	Authorization required for disclosure of nonpublic health information (Insurance)	Statute prohibits a licensee from disclosing nonpublic personal health information about a consumer to a third party without authorization.
	Pa. Admin. Code Tit. 31 § 146b.11	Authorization required for disclosure of nonpublic health information	Licensees may not disclose nonpublic health information about a consumer without authorization.
	40 Pa. Stat. Ann. §§ 991.2101, 991.2131(a), 991.2152(a)(2)	Quality healthcare accountability and protection (HMOs)	HMOs are required to adopt and maintain procedures to ensure that all identifiable information regarding enrollee health, diagnosis and treatment is adequately protected and remains confidential.
Rhode Island	R.I. Gen. Laws § 5-37.3-4	The Confidentiality of Health Care Communications and Information Act — Limitations on and permitted disclosures	Provides for a general, comprehensive prohibition against disclosure of confidential health care information.

State	Statue (Citation)	Title of Statute	Comments
	R.I. Regs. R. 02-030-100	Privacy of Consumer Information	Licensees may not disclose nonpublic health information without consumer authorization subject to a few exceptions.
	R.I. Gen. Laws § 27-41-22	Statutory construction and relation to other laws (HMOs)	HMOs may not release or transfer confidential health care information, including a subscriber's health care history, diagnosis, condition, treatment, or evaluation except under provisions of the Confidentiality of Health Care Communications and Information Act.
	R.I. Gen. Laws § 27-18-52.1	Accident and Sickness Insurance Policies — Genetic information	Regarding confidentiality of genetic information.
	R.I. Gen. Laws § 40.1-5-26	Mental Health Law — Disclosure of confidential information and records.	Regarding confidentiality of health information (mental health).
South Carolina			No general/comprehensive prohibition on disclosure of medical information.
	S.C. Code Ann. § 44-115-130	Physicians' Patient Records Act — Sale of medical records by physician restricted; notice of intent to sell	Statute limits the sale/transfer of medical records by physicians, and establishes a process for sale of records to other South Carolina licensed physicians, osteopaths or hospitals.
	S.C. Code Ann. § 44-115-40	Physician not to release records without express written consent	Statute prohibits physician from releasing medical records without express written consent.
	S.C. Code Ann. Regs. 69-58	Privacy of Consumer Financial and Health Information (Insurance)	Regulation governs the treatment of nonpublic personal health information. Compliance with HIPAA pre-empts the statutory requirements. Regulation applies to HMOs.

State	Statue (Citation)	Title of Statute	Comments
	S.C. Code Ann. § 38-33-260	Confidentiality of health records (HMOs)	Any health data obtained by an HMO is confidential and may not be disclosed without consent unless authorized.
	S.C. Code Ann. Regs. 61-93	Record Maintenance [for Facilities that Treat Individuals for Psychoactive Substance Abuse or Dependence]	Regarding confidentiality of records (substance abuse).
	S.C. Code Ann. Regs. 126-170	Department of Health and Human Services — Safeguarding of client information - General	Regarding records maintained in connection with any federally assisted alcohol or drug abuse program; information from programs and grants administered by the Commission.
	S.C. Code Ann. § 44-44-100	South Carolina Birth Defects Act — Use and disclosure of birth defects data	Birth defects data may be used and disclosed for the purposes of scientific research concerning causation, prevention strategies, epidemiological analysis, environmental and geographic study, and other purposes authorized by the department.
	S.C. Code Ann. § 44-22-100	Rights of Mental Health Patients — Confidentiality of records; exceptions; violations and penalties	Restricts provider disclosure of health information (mental health).
South Dakota			No general/comprehensive provisions governing confidentiality of health care data.
	S.D. Admin. R. § 44:04:09:04	Written policies and confidentiality of records	Providers are required to establish written policies and procedures to govern the administration and activities of the medical record service.

State	Statue (Citation)	Title of Statute	Comments
	S.D. Codified Laws § 58-2-40	Division of Insurance	Law directs the director of insurance to promulgate rules pursuant to chapters 1-26, to protect the privacy of personally identifiable health care and medical information, data, and records.
	S.D. Codified Laws § 58-41-125	Insurance — Health maintenance organizations — Confidentiality of information	Information provided to the director by an HMO relative to risk bearing entities is confidential. HMOs have privilege under S.D. Codified Laws § 58-41-78.
	S.D. Admin. R. 20:06:45:27	Disclosure of nonpublic personal health information	Licensee may not disclose nonpublic personal health information absent authorization. Exceptions include disclosures permitted without authorization under HIPAA.
	S.D. Admin. R. 46:05:07:02	Guaranteed Rights	A client has rights including... (4) The right to confidentiality of all records, correspondence, and information relating to assessment, diagnosis, and treatment in accordance with 42 U.S.C. §§ 290 dd-2 and 42 C.F.R. Part 2 (June 9, 1987), and 45 C.F.R. Parts 160 and 164 (April 17, 2003).
	S.D. Codified Laws § 34-22-12.1	Contagious Disease Control — Confidentiality of reports; exceptions	Regarding immunization records.
	S.D. Codified Laws §§ 27A-12-25, 27A-12-26, 27A-12-32	Individual records required-contents-confidentiality	Restricts provider disclosure of health information (mental health).
Tennessee			No general/comprehensive provisions governing confidentiality of health care data.

State	Statue (Citation)	Title of Statute	Comments
	Tenn. Code Ann. § 63-2-101	Release of medical records — Definitions	Statute generally restricts disclosure of the name and address and other identifying information of a patient. The name and address and other identifying information shall not be sold for any purpose. Any violation of this provision is deemed an invasion of the patient's right to privacy. Except as otherwise authorized... a provider shall have a policy to protect the dignity of a patient... by limiting the use and disclosure of medical records... even if the patient's information is de-identified.
	Tenn. Code Ann. § 68-11-1503	Confidentiality	The name and address and other identifying information shall not be sold for any purpose.
	Tenn. Comp. R. & Regs. R. 0780-1-72-.11	Limits on disclosure of nonpublic personal information to nonaffiliated third parties	Licensee prohibited from disclosing nonpublic personal information to nonaffiliated third parties without consumer authorization.
	Tenn. Code Ann. §§ 56-7-2701; 56-7-2704	Genetic Information Nondisclosure in Health Insurance Act of 1997	Statute prohibits insurance providers from disclosing genetic information.
	Tenn. Code Ann. § 56-32-125	Confidentiality of information (HMOs)	Statute prohibits HMOs from disclosing data or information related to diagnosis, treatment or health without express written consent.
	Tenn. Code Ann. § 33-10-408	Requirements for confidentiality of substance abuse treatment records	Regarding testing/information (hepatitis B virus and the HIV virus, other STD or tuberculosis status).
	Tenn. Code Ann. § 33-3-103	Confidentiality of mental health records	Regarding disclosure of mental health information.

State	Statue (Citation)	Title of Statute	Comments
	Tenn. Code Ann. § 68-1-1006	Cancer Reporting System; Confidentiality	Regarding disclosure of cancer information.
Texas			No general/comprehensive prohibition on disclosure of confidential health care data.
	Tex. Ins. Code Ann. §§ 602.001, 602.051, 602.053 (2011)	§ 602.001 Definitions §602.051 Authorization for Disclosure of Certain Health Information § 602.053 Exceptions	Covered entities can generally not disclose without consent, except as permitted, including any activity that permits disclosure without authorization under HIPAA. Insurers and HMOs are considered "covered entities."
	Tex. Health & Safety Code § 181.152	Marketing Uses of Information	A covered entity must obtain clear and unambiguous written or electronic form to use or disclose protected health information for any marketing communication, with exceptions.
	Tex. Health & Safety Code § 181.153	Sale of Protected Health Information Prohibited; Exceptions	A covered entity may not disclose an individual's protected health information in exchange for direct or indirect remuneration except to another covered entity for treatment, payment, insurance or health care function.
	Tex. Admin. Code Tit. 28, § 222.53	Authorization Required for Disclosure of Nonpublic Health Information	Covered entity required to obtain authorization prior to disclosure of nonpublic health information.
	Tex. Ins. Code Ann. § 843.007	Confidentiality of Medical and Health Information (HMOs)	Confidentiality provisions apply with respect to medical and health information obtained by HMOs. HMOs may not disclose enrollees' treatment, diagnosis or health information without express consent.

State	Statue (Citation)	Title of Statute	Comments
	Tex. Health & Safety Code § 611.002	Confidentiality of Information and Prohibition Against Disclosure	Communications between a patient and a professional, and records of the identity, diagnosis, evaluation, or treatment of a patient that are created or maintained by a professional, are confidential.
	Tex. Health & Safety Code § 611.004	Authorized Disclosure of Confidential Information Other than in Judicial or Administrative Proceeding	Regarding disclosure of confidential information by professionals.
	Tex. Health & Safety Code Ann § 87.002	Confidentiality	Except as specifically authorized, information furnished to a department employee or agent that relates to cases or suspected cases of a health condition are confidential.
	Tex. Health and Safety Code §§ 611.002, 611.004	Confidentiality of Information and Prohibition Against Disclosure	Restricts provider disclosure of health information (mental health).
	Tex. Health and Safety Code §§ 595.001, 595.003, 595.005, 595.008, 595.009	Persons with Mental Retardation Act	Restricts provider disclosure of health information maintained in connection to a program or activity related to mental retardation.
	Tex. Health and Safety Code § 533.010	Information relating to patient's condition	Concerning disclosure of health information (mental health) by the department or a medical organization, hospital or hospital committee, including in connection with research.
	Tex. Health and Safety Code § 82.009	Confidentiality (cancer)	Data furnished to a cancer registry or a cancer researcher is for the confidential use of the cancer registry or the cancer researcher.

State	Statue (Citation)	Title of Statute	Comments
Utah			No general/comprehensive provisions governing confidentiality of health care data.
	Utah Admin. Code R. 590-206-17	When Authorization Required for Disclosure of Nonpublic Personal Health Information	Insurers and HMOs are prohibited from disclosing a consumer or customer's nonpublic personal health information without the individual's authorization.
	Utah Code Ann. § 26-6-27	Utah Communicable Disease Control Act — Information regarding communicable or reportable diseases confidentiality; exceptions	Concerning confidentiality of health information (communicable diseases).
Vermont	Vt. Stat. Ann. Tit. 18 § 1852 -1854	Patients' bill of rights; adoption	A patient has the right to expect that all communications and records pertaining to his or her care shall be treated as confidential. Only medical personnel, or individuals under the supervision of medical personnel, directly treating the patient, or those persons monitoring the quality of that treatment, or researching the effectiveness of that treatment, shall have access to the patient's medical records. Others may have access to those records only with the patient's written authorization. Separate statutes govern the confidentiality of nursing home residents' personal and medical records (Vt. Stat. Ann. tit. 33 § 7301) and prescriptions, orders and records (Vt. Stat. Ann. tit. 18 § 4211).
	Vt. Code R. 21-010-016	Privacy of Consumer Financial and Health Information Regulation	Regulation restricts disclosure of nonpublic health information.

State	Statue (Citation)	Title of Statute	Comments
	Vt. Code R. 21-020-053, § 9	Insurance Division — Privacy of consumer financial and health information regulation	Statute prohibits licensee from disclosing nonpublic personal information.
	Vt. Stat. Ann. Tit. 18 § 7103	Health – General provisions - Disclosure of information	All certificates, applications, records, and reports … directly or indirectly identifying a patient or former patient or an individual whose hospitalization or care has been sought or provided under this part, together with clinical information relating to such persons shall be kept confidential without consent unless an exception is met.
	Vt. Stat. Ann. Tit. 18 § 7103	Disclosure of information	Restricts provider disclosure of health information (mental health).
Virginia	Va. Code Ann. § 32.1-127.1:03(A)(1) & (3)	Health Records Privacy Act	Statute prohibits disclosure of an individual's record by a health care entity or a person working in a health care setting without the individual's authorization. Broad protections provided.
	Va. Code Ann. § 2.2-3705.5	Exclusions to application of chapter; health and services records	Statute exempts health records from disclosure under the state Freedom of Information Act with certain exceptions.
	Va. Code Ann. § 38.2-613	Disclosure limitations and conditions [Insurance Information and Privacy Protection]	Insurers may not disclose any medical record information without proper written authorization.
	Va. Code Ann. §§ 38.2-601 and 602	Insurance Information and Privacy Protection [Application of chapter]	Insurance institutions are covered by the Virginia Insurance and Privacy Protection Act. HMOs under the definition of "insurance institution" are covered by the Virginia Insurance and Privacy Protection Act.

State	Statue (Citation)	Title of Statute	Comments
	Va. Code Ann. § 32.1-70	Information from hospitals, clinics, certain laboratories and physicians supplied to Commissioner; statewide cancer registry.	Regarding disclosure of cancer information.
	Va. Code Ann. § 32.1-36.1	Confidentiality of test for human immunodeficiency virus; civil penalty; individual action for damages or penalty	Concerning disclosure of HIV/AIDS related information.
Washington	Wash. Rev. Code § 70.02.020.050	Medical Records — Health Care Information Access and Disclosure	No disclosure by health care providers except as authorized without consent. Exceptions include disclosure of a limited data set that excludes direct identifiers. Disclosure without authorization permitted for limited purposes, including [among other things] for use in a research project in accordance with institutional review board guidelines.
	Wash. Rev. Code § 70.02.030	Medical Records — Health Care Information Access and Disclosure	Unless otherwise provided, an authorization may permit the disclosure of health care information to a class of persons that includes… researchers with informed consent.
	Wash. Rev. Code § 70.02.045	Medical Records — Health Care Information Access and Disclosure (Insurance)	"Third-party payors shall not release health care information disclosed under this chapter, except to the extent that health care providers are authorized to do so under RCW 70.02.050." HMOs are included in the definition of third-party payors. Wash. Rev. Code Ann. § 70.02.010(43).
	Wash. Rev. Code § 70.47.150	Health Care Access Act — Confidentiality	Records obtained, reviewed by, or on file with the plan are exempt from public inspection and copying.

State	Statue (Citation)	Title of Statute	Comments
	Wash. Rev. Code § 70.96A.150 (2012)	Records of alcoholics and intoxicated persons	Regarding confidentiality of records of treatment programs.
	Wash. Rev. Code §§ 71.05.390; 71.05.630	Confidential information and records — disclosure	Restricts provider disclosure of health information (mental health).
West Virginia			No general/comprehensive provision governing confidentiality of health care data.
	W. Va. Code R. § 114-57-18	Relationship to Federal Rules	Licensee compliance with HIPAA satisfies requirements.
	W. Va. Code R. § 114-57-15 to 17	Privacy of Consumer Financial and Health Information (Insurance)	Rule regulates licensees disclosure of nonpublic personal health information.
	W. Va. Code Ann. § 33-25A-26	Confidentiality of medical information (HMOs)	Information relating to enrollee's diagnosis, treatment, or health is confidential unless express written consent provided by enrollee.
	W. Va. Code Ann. § 16-3C-1	Public Health — Aids-related medical testing and records confidentiality act	Concerning disclosure of HIV/AIDS-related information.
	W. Va. Code Ann. § 27-3-1	Definition of confidential information; disclosure (mental health)	Restricts provider disclosure of health information (mental health).

State	Statue (Citation)	Title of Statute	Comments
Wisconsin	Wis. Stat. § 146.82	Notice	All patient health care records shall remain confidential. Permissible uses include research, subject to conditions described. Disclosure is also permitted if the patient health care records do not contain information and the circumstances of the release do not provide information that would permit the identification of the patient.
	Wis. Stat. § 610.70 (5)	Disclosure of personal medical information (Insurance)	Any disclosure by an insurer of personal medical information concerning an individual shall be consistent with the individuals signed disclosure authorization form, unless an exception is met. Wis. Stat. Ann. § 610.70 definition of insurers [§600.03 (23c)] includes HMOs.
	Wis. Adm. Code Ins. § 25.70	When authorization required for disclosure of nonpublic personal health information	Licensee is prohibited from disclosing nonpublic personal health information without consumer or customer authorization.
	Wis. Stat. § 51.30	Records	Restricts provider disclosure of health information (mental health).
	Wis. Stat. § 255.04 (2012)	Cancer Reporting	Regarding disclosure of cancer information.
	Wis. Stat. § 51.30 (2012)	Birth defect prevention and surveillance system	Regarding disclosure of information (birth defects/treatment).
Wyoming			No general/comprehensive provisions governing confidentiality of health care data.

State	Statue (Citation)	Title of Statute	Comments
	Wyo. Stat. Ann. § 35-2-606; 35-2-609	§ 35-2-606 Disclosure of health care information by hospital § 35-2-609 Disclosure without patient's authorization	A hospital (or its agent or employee) shall not disclose any hospital health care information about a patient to any other person without the patient's written authorization under Wyo. Stat. Ann. § 35-2-606, unless authorized under Wyo. Stat. Ann. § 35-2-609.
	044-000 Wyo. Code R. §54	Privacy of Consumer Financial and Health Information (Insurance)	Licensed insurance entities are generally restricted from disclosure of nonpublic personal health information about a consumer or customer, unless a specific exception is met or otherwise permitted under HIPAA.
	Wyo. Stat. Ann. § 26-34-130	Confidentiality of medical information (HMOs)	Statute requires health maintenance organizations to hold in confidence data or information pertaining to the diagnosis, treatment or health of any enrollee or applicant.
	Wyo. Stat. Ann. § 25-10-122; HEA-MHSA 6 Wyo. Code R. § 4	Records to be kept confidential; exceptions	Restricts provider disclosure of health information (mental health).

For additional information, please contact **Beni Surpin** at 858.847.6736 or bsurpin@foley.com

About Foley

Foley & Lardner LLP provides award-winning business and legal insight to clients across the country and around the world. Our exceptional client service, value, and innovative technology are continually recognized by our clients and the legal industry. Foley has been recognized in a survey of *Fortune* 1000 corporate counsel as an elite BTI Client Service 30 — one of only seven law firms to hold this distinction for more than 12 years (2015 BTI Client Service A-Team survey, The BTI Consulting Group, Wellesley, MA). In addition, Foley received 27 national Tier 1 rankings in the 2015 edition of U.S. News – Best Lawyers® "Best Law Firms," and was named to the *InformationWeek* 500 list for seven of the past eight years for technological innovation that enhances business value. At Foley, we strive to create legal strategies that help you meet your needs today — and anticipate your challenges tomorrow.

Foley.com

Best Lawyers® BEST LAW FIRMS U.S.News & WORLD REPORT 2015

FOLEY

FOLEY & LARDNER LLP

BOSTON · BRUSSELS · CHICAGO · DETROIT · JACKSONVILLE · LOS ANGELES · MADISON · MIAMI · MILWAUKEE · NEW YORK · ORLANDO · SACRAMENTO
SAN DIEGO · SAN FRANCISCO · SHANGHAI · SILICON VALLEY · TALLAHASSEE · TAMPA · TOKYO · WASHINGTON, D.C.