THE SOURCE
ON HEALTHCARE PRICE & COMPETITION

A Source white paper

All-Payer Claims Databases: The Balance Between Big Healthcare Data Utility and Individual Health Privacy

ANDREW KELLY, PhD and JAIME KING, JD, PhD

October 2017

UCSF/UC Hastings Consortium on Law, Science and Health Policy

EXECUTIVE SUMMARY

As policymakers pursue the Triple Aim of reducing costs, improving quality, and expanding access, the development of an All-Payer Claims Database (APCD) can provide invaluable information about the drivers of cost, the value of health care interventions, and the efficacy of policy initiatives. APCDs collect and store patient and provider-specific claims data including the amounts paid by payers throughout the state. The popular quote, "you can't manage what you can't measure" is nowhere more applicable than in the American healthcare system. To achieve the Triple Aim, both California and the nation must measure and understand healthcare prices and utilization patterns throughout the complex healthcare system. Furthermore, as consumer-directed health initiatives, such as high deductible health plans and health savings accounts, proliferate and provide patients with greater personal risk in health care decision-making, consumers will demand greater access to price and quality information for comparison. All-Payer Claims Databases form the foundation for the development of price and quality transparency tools, and offer a means of providing critical information in a timely manner for patients, policymakers, and health services researchers.

The data collected by APCDs, however, also contains information that individuals, providers, and insurers would like to remain confidential. Given the sensitivity of individual health information contained in claims data, any database collecting, storing, and disseminating such information must ensure adequate privacy and security for all patient information. Furthermore, a web of federal and state privacy laws that govern the use, storage, and disclosure of information from an APCD must be untangled to determine the privacy requirements that each APCD must attain.

This report examines the balance policymakers in California must strike between providing the necessary access to healthcare price and utilization data to improve healthcare decision-making and protecting confidential health information. Part I of the report provides a brief background on APCDs and their current usage. Part II examines California's failed attempt to pass SB 1159 in 2016, and the existing data privacy regulations that would govern any future attempt to create an APCD in the state.

Part III of this Report analyzes four state APCDs to gauge the variety of state privacy and security procedures. It examines the structure and policy of existing APCDs in Maine, Massachusetts, and Colorado, as well as the development of the New York APCD. After reviewing the implementing legislation and regulations for each APCD, we defined three areas as key to establishing sound privacy and security procedures - the governance structures and oversight institutions, the security measures, and the disclosure requirements and processes. Policy choices in each of these three areas determine how states balance the utility of access to APCD-housed information and protection of private health information. Our recommendations for legislation implementing an APCD in California are divided into three categories: A) governmental oversight and structure; 2) data privacy and security; and 3) release of information. These recommendations are included at the conclusion of the description and analysis of the four states, as well as summarized below.

Recommendations:

Governance Structures and Oversight Institutions

The design of an APCD's governance structure and oversight capacity can promote transparency and accountability, while also extending the administrative and operational capabilities of the ACPD. The state APCDs vary on several factors related to governance structure and oversight capacity: the permanence of the oversight bodies, the oversight bodies' membership, and the governance and operational responsibilities given to the oversight body. States can design these structures in ways that promote continued enhancement of data protection and security measures within the APCD.

We recommend the creation of an independent, permanent oversight body with a broad-based membership that requires both representation from specific stakeholder groups, including patient advocates, provider organizations, payers, small and large employers, members of the state legislature, and advocates for protection of individual data on the internet, as well as individuals with expertise critical to the operation of an APCD, including data privacy and security experts, academic researchers, and health economists.

We recommend that California collect data in accordance with the Common Data Layout, to maximize compatibility with other state data for comparison and analysis.

We also recommend shared appointment power, as Massachusetts has done, with various entities possessing the ability to appoint members to the oversight body. Finally, the state legislature should provide some restrictions on which entities the oversight body can contract with and ensure those entities are subject to the relevant data privacy laws and protections. If California allows the oversight body to contract with any type of entity, we recommend requiring each contracting entity provide ongoing proof that it has significant data privacy and security measures in place for the duration of the contract. Finally, the governance structure and oversight procedures would also benefit from the inclusion of clear legislative language regarding the binding or non-binding nature of any recommendations issued by the advisor committee.

Privacy and Security Protections

Data collected, stored, and maintained by an APCD is highly sensitive and personal, requiring strong protections against breach and theft. Concerns regarding the centralization of such data within a single entity, particularly given the prevalence of cyber-attacks and the recent targeting of health care systems and hospitals, are both understandable and reasonable. The four states took significant measures to ensure the security and confidentiality of claims data submitted to their APCD.

We recommend that California follow Colorado's approach and include legislative language that specifically subjects the APCD to the Health Information Portability and Accountability Act (HIPAA) and the California Medical Information Act (CMIA). As a government entity, an APCD is not considered a

"covered entity" under HIPAA or CMIA, and, therefore, would not be required to follow either HIPAA's or CMIA's security and privacy requirements. This approach would establish HIPAA and CMIA as the minimum, "floor" level for security and privacy procedures, but would allow the legislature or the Secretary of CHHSA and the APCD oversight body to establish additional requirements and procedures to supplement the privacy foundations created by HIPAA and CMIA. Further, incorporating well known and understood privacy and security requirements like those included in HIPAA and CMIA provides assurances to patients and their advocates that their data will be protected by measures they are accustomed to, without requiring the legislature or the oversight body to draft and consistently update an entirely new set of regulations.

Data Release

The release of data that simultaneously allows for the critical analysis of the health care system and ensures data security and patient privacy is the central task of any APCD. To achieve this primary function, those overseeing the APCD must establish a clear and robust set of procedures to govern the collection, maintenance, storage, and release of APCD data. State legislation varies in regards to the restrictions placed on the release of de-identified and identifiable data. Some states specify a particular set of purposes for which data can be released, as well as identify different types of data that can only be requested by certain categories of requestors. Other states, however, have enacted legislation that provides only minimal criteria for the collection, maintenance, storage, and release of data. Such states give considerable discretion and authority to executive directors or administrators to establish privacy and security protections through regulations. Another key structural difference among states that can impact security and privacy is the extent to which legislation allows for the contracting out of APCD activities to a third-party. The variation among states reviewed here ranges from a complete prohibition in Massachusetts to New York's permissive structure that allows the commissioner to contract out *any* APCD activity. In addition to variations in the procedures and protections for data security and privacy, the states also vary significantly in the clarity and specificity with which legislative language addresses these critical APCD functions.

We recommend that the California legislation make the release of APCD data subject to HIPAA and CMIA. As was true for security and privacy procedures, HIPAA and CMIA would set only the minimum restrictions and requirements for the release of APCD data. The California legislature or the Secretary, acting with input from the advisory committee, could then enact or issue additional APCD-specific data release provisions that would establish stronger protections and more rigorous procedures for the release of data.

Both HIPAA and CMIA establish broad constraints on the disclosure or release of personal medical information without the authorization of the patient in question. HIPAA and CMIA, however, also establish exceptions that allow for the disclosure of PHI in the absence of authorization from the affected patient. The exceptions include disclosures required by law and for certain research purposes, with the latter subject to additional constraints and data safety requirements. Under CMIA, the provisions restricting the re-disclosure of medical information would apply to any entity or person that receives data from the APCD.

We also recommend that legislation include a direct and explicit discussion of de-identified and identifiable data. Among the states reviewed here, legislation often created unnecessary confusion as a result of legislative language that did not clearly establish an explicit demarcation between the different approaches to identifiable and de-identified data. We further recommend that the legislation specifically outline the categories of actors that may request identifiable and de-identified APCD data, as well as specify the purposes for which data may be requested. The legislation should also provide individuals the opportunity to opt out of having their identifiable data released for research without their consent. To add additional oversight and protections for the release of identifiable data, we recommend establishing a committee to oversee and review requests for identifiable data.

Overall, we recommend that California establish an All Payer Claims Database designed to collect all health care claims data within the state to promote transparency, informed decision making, and improve health and healthcare for all Californians. We recommend that the legislature do so in a manner that provides robust protection for personal health information while enabling policymaker, researchers, and public health authorities reasonable access to the data collected by the APCD to promote improvements in health and health care throughout the state. We recommend an independent oversight body with a broad membership appointed by a range of individuals and organizations to ensure diversity and expertise within its membership. At a minimum, the legislature should subject the APCD to the requirements of HIPAA and CMIA, as though it were a covered entity. These requirements provide a solid baseline for privacy protections, while granting the oversight body or the Department of Health and Human Services the option to increase the stringency of the requirements as needed.

Authors and Acknowledgments

Andrew S. Kelly, PhD
Assistant Professor (Effective Fall 2017)
Health Sciences Program
California State University, East Bay
25800 Carlos Bee Blvd
Hayward, CA 94542
andrewkellyphd@gmail.com

Jaime S. King, JD, PhD
Professor of Law
University of California, Hastings College of the Law
Associate Dean and Co-Director
UCSF/UC Hastings Consortium on Law, Science, and Health Policy
Executive Editor
The Source on Healthcare Price and Competition
200 McAllister St.
San Francisco, CA 94102
(415) 581-8834 (office)
kingja@uchastings.edu

Acknowledgments

The authors would like to thank the California Health Care Foundation for its support of the research contained herein.

The authors would also like to thank Carson Dudley and Anna Zaret for their valuable research assistance on this project.

Table of Contents

Introduction

In 2015, healthcare spending in the United States accounted for 17.8% of the national economy.[1] The $3.2 trillion price tag for national health expenditure equates to $9,990 per person.[2] In 2014, the most recent year in which state-level spending data is available, California's per capita health expenditure was $7,549—just below the national average of $8,045.[3] These figures place U.S. healthcare spending above that of any other advanced industrial country, both as percentage of GDP and on a per capita basis. There is, in fact, not a single country that comes close to U.S spending levels. France, with a national health expenditure of 11.6% of GDP, and Switzerland, with per person expenditures of $6,325, are the closest competitors on either measure.[4] In their groundbreaking article, "It's the Prices, Stupid," Gerard Anderson, Uwe Reinhardt, and their colleagues compared spending across OECD nations, concluding that U.S. spending was not driven by higher utilization, but, as their title implies, healthcare spending in U.S. is driven by the higher prices paid for comparable services in the U.S.[5] Despite recent slowdowns in healthcare spending, the growth rate has remained positive and kept the U.S. on an unsustainable path of healthcare spending. The current spending levels threaten the solvency of American families, businesses, and federal and state governments.

As policymakers pursue the Triple Aim of reducing costs, improving quality, and expanding access, the development of an All-Payer Claims Database (APCD) can provide invaluable information about the drivers of cost, the value of health care interventions, and the efficacy of policy initiatives. APCDs collect and store patient and provider-specific claims data including the amounts paid by payers throughout the state. The popular quote, "you can't manage what you can't measure" is nowhere more applicable than in the American healthcare system. To achieve the Triple Aim, both California and the nation are going to have to measure and understand healthcare prices and utilization patterns throughout the complex healthcare system. Furthermore, as consumer-directed health initiatives, such as high deductible health plans and health savings accounts, proliferate providing patients with greater

---

[1] Center for Medicare and Medicaid Services, National Health Expenditures Fact Sheet, available at: https://www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata/nhe-fact-sheet.html.

[2] Id.

[3] Kaiser Family Foundation, Health Care Expenditures Per Capita by State of Residence, available at: http://www.kff.org/other/state-indicator/health-spending-per-capita/?currentTimeframe=0&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D.

[4] David Squires and Chloe Anderson, "U.S. Health Care from a Global Perspective: Spending, Use of Services, Prices, and Health in 13 Countries." The Commonwealth Fund, October 2015, available at http://www.commonwealthfund.org/~/media/files/publications/issue-brief/2015/oct/1819_squires_us_hlt_care_global_perspective_oecd_intl_brief_v3.pdf

[5] Gerard F. Anderson, Uwe E. Reinhard, Peter S. Hussey, and Varduhi Petrosyan, "It's the Prices, Stupid: Why The United States Is So Different From Other Countries." *Health Affairs* 22 (3): 89-105.

personal risk in health care decision-making, consumers will demand greater access to price and quality information for comparison. All-Payer Claims Databases form the foundation for the development of price and quality transparency tools, and offer a means of providing critical information in a timely manner for patients, policymakers, and health services researchers.

The data collected by APCDs, however, also contains information that individuals, providers, and insurers would like to remain confidential. Given the sensitivity of individual health information contained in claims data, any database collecting, storing, and disseminating such information must ensure adequate privacy and security for all patient information. Furthermore, a web of federal and state privacy laws that govern the use, storage, and disclosure of information from an APCD must be untangled to determine the privacy requirements that each APCD must attain.

This report examines the balance policymakers in California must strike between providing the necessary access to healthcare price and utilization data to improve healthcare decision-making and protecting confidential health information. Part I of the report provides a brief background on APCDs and their current usage. Part II examines California's failed attempt to pass SB 1159 in 2016, and the existing data privacy regulations that would govern any future attempt to create an APCD in the state. Part III examines the policies and practices governing APCDs in four other states - Maine, Massachusetts, Colorado, and New York - to identify suggested practices for California regarding data privacy, security, and dissemination. Finally, Part IV summarizes these recommendations.

I. All Payer Claims Databases

What is an APCD?

All-Payer Claims Databases (APCDs) are electronic database systems that collect and aggregate health care data derived from medical, dental, and pharmacy claims from third-party payers.[6] This data includes information about healthcare prices, quality, and utilization. The majority of existing APCDs are mandated by state law, with reporting statutes requiring the submission of claims data to a state collecting agency. Due to the unavailability of claims data and preemption from state regulations relating to some employee benefit plans by the Employee Retirement Income Security Act (ERISA), data from self-insured employers and uninsured patients are not typically included in APCDs and are not subject to state reporting statutes.[7]

According to the APCD Council (a collaboration between the University of New Hampshire and the National Association of Health Data Organizations), 15 states have existing APCDs, with 5 more in

[6] For the purposes of data collection, a third-party payer may include private insurers, third-party administrators, pharmacy and dental benefit administrators, Medicaid, Medicare, the Federal Employees Health Benefit Program, and TRICARE.

[7] Erin C. Fuse Brown and Trish Riley, Empowering and Protecting Consumers: ERISA Thwarts State Innovation, available at http://nashp.org/empowering-and-protecting-consumers-erisa-thwarts-state-innovation/.

implementation as of July 2017.[8] APCDs can also be created voluntarily. For example, The California Healthcare Performance Information System ("CHPI"), a public benefit corporation, administers a voluntary APCD that consists of claims from Medicare fee-for-service, Anthem Blue Cross, Blue Shield of California, and United Healthcare.[9] There are currently 5 states with these types of voluntary APCD efforts.[10]

Although no uniform nationwide data collection requirements exists in the U.S., states generally collect the following information: (1) patient social security number or member ID; (2) type of care plan and contract; (3) patient demographics; (4) diagnosis/treatment code or drug code; (5) service provider information; (6) member payment responsibility; (7) type and date of bill paid; (8) facility type; (9) revenue codes; and (10) services dates.[11] The ability to collect and maintain this data from providers and payers across fragmented healthcare systems makes APCDs a unique tool in the fight to lower costs, improve quality, and increase access. Since the Supreme Court decision in *Gobeille,* the APCD Council, representative states, and several other stakeholders have worked extensively to develop the Common Data Layout, a uniform, standardized set of health care claims and related data elements that could be used across states, the Department of Labor, and APCDs.[12] Use of the Common Data Layout minimizes the burden on policymakers determining what data to collect, payers submitting data in different states, and researchers looking to standardize data for analysis.

Why is an APCD Needed?

By collecting and aggregating claims information, APCDs help make healthcare data more easily accessible to policymakers, researchers, and consumers. If price information and quality measures remain fragmented and largely obscured, policymakers and consumers will only possess a vague and incomplete understanding of the health care environment. As a result, both patient decisions and efforts at comprehensive delivery and payment reform will be guided by incomplete information.

APCDs Inform Policy and Health Reform

APCDs allow states to monitor utilization and healthcare charges across third-party payers, which enables researchers and policymakers to identify and respond to systematic delivery and payment

---

[8] APCD Counsel, Interactive State Report Map, available at https://www.apcdcouncil.org/state/map.

[9] California Healthcare Performance Information System, Multi-Payer Claims Database, available at http://www.chpis.org/programs/mpcd.aspx.

[10] APCD Counsel, Interactive State Report Map, available at https://www.apcdcouncil.org/state/map.

[11] National Association of Health Data Organizations, APCD Factsheet (2010), available at https://www.nahdo.org/sites/nahdo.org/files/Resources/APCD%20Fact%20Sheet_FINAL_2.pdf.

[12] Nat'l Academy of State Health Pol'y, Comments on Department of Labor Notice of Proposed Rulemaking, September 20, 2016, available at https://www.dol.gov/sites/default/files/ebsa/laws-and-regulations/rules-and-regulations/public-comments/1210-AB63/00030.pdf.

trends among many settings. APCDs also enable policymakers to monitor the impact and effectiveness of policy reforms and innovations at each phase of implementation. Legislators and regulators can then evaluate and improve upon state healthcare cost reduction strategies and delivery reform in an efficient manner.

APCDs also allow states to team with researchers to study healthcare cost variation, population health, and utilization. Colorado has particularly made significant strides towards realizing the potential of APCD resources for researchers. Colorado's APCD permits organizations to promulgate customized data requests for projects to further health outcomes, lower costs, and improve quality of care.[13] Colorado has launched a showcase of ways research organizations (predominantly non-profits and state government) are using customized data sets in the areas of health coverage and rate setting, outcome/cost improvement, and payment reform. Projects of note include a study to determine whether home-delivered meals to chronically ill patients will reduce overall healthcare expenditures;[14] a study on reducing cesarean delivery rates;[15] a study to find ways to increase use of non-opioid perioperative painkillers to reduce opioid prescriptions;[16] and a study by an orthopedic care provider to investigate opportunities to implement bundled payments as an alternative for fee-for-service.[17] Other APCD states are working towards linking clinical data from provider health information exchanges and plan design from health insurance exchanges to study the linkages between clinical outcomes and plan design on spending. As these projects demonstrate, the comprehensive data collected by APCDs can help inform researchers and states working on a variety of healthcare improvement initiatives.

Furthermore, access to a comprehensive database of healthcare cost and utilization data has become increasingly important to state policymakers as recent federal reforms have devolved more healthcare policy decisions, as well as more opportunities for innovation, to the state level. In California, for example, the ACA has resulted in more than 3.8 million more people gaining MediCal

---

[13] Center for Improving Value in Health Care, CO APCD Annual Report 2016, available at http://www.civhc.org/getmedia/80881590-f979-41b2-89dd-cb2bdaeb5424/FINAL-2016-CO-APCD-Annual-Report-with-Bookmarks.pdf.aspx/.

[14] CO Medical Price Compare Data Showcase, Project Angel Heart (Nutrition & Chronic Conditions) available at http://www.comedpriceshowcase.org/portfolio/project-angel-heart/.

[15] Center for Improving Value in Health Care, Opportunities to Bend the Cost Curve: Reduce Cesarean Delivery Rates in Colorado (July 2014), available at http://www.civhc.org/getmedia/dbe5c38b-fa8a-49f2-a142-36d910a860ff/C-section-APCD-Analysis.pdf.aspx/.

[16] CO Medical Price Compare Data Showcase, University of Colorado, Dept. of Anesthesiology (Perioperative Painkillers), available at http://www.comedpriceshowcase.org/portfolio/uc_anesthesiology/.

[17] CO Medical Price Compare Data Showcase, Healthcare Provider (Orthopedic Bundles), available at http://www.comedpriceshowcase.org/portfolio/p32/.

eligibility.[18] MediCal now accounts for 27% of state spending in California,[19] creating an even greater impetus and need to track statewide spending and utilization data through an APCD. The ability to track health care spending both across time and geographic area will prove invaluable to cost containment within this vital program. States like Massachusetts have successfully employed an APCD and its related capacities to set spending targets that have helped control costs. In addition, Massachusetts, along with Minnesota, Oregon, Maine, Vermont, and Arkansas have all relied on the capacities of their existing APCDs to help secure State Innovation Model grants and implement and assess cutting-edge delivery and payment reforms.

Regardless of the direction health care reform proceeds under the current Republican White House and Congress, states will become increasingly important players in the development and implementation of healthcare reform. If Republicans succeed in transforming Medicaid from an open-ended entitlement to a block grant or per capita cap funding structure, California, if it chooses to maintain current MediCal benefit levels and enrollment, will become responsible for a significantly increased level of expenditures, requiring innovative policy reforms and an increased focus on cost containment and utilization. If, on the other hand, California attempted to establish a single-payer model for the state, understanding healthcare spending and utilization patterns across the state will prove essential to policy design and implementation. In both scenarios, and for everything in between, California will require the type of data collection and analysis that an APCD makes possible.

APCDs Empower Consumers

APCDs not only empower policymakers to create innovative solutions to health care challenges, but they can also empower consumers to become better purchasers and participants in their own care. The rise of High Deductible Health Plans (HDHPs) has placed a considerable burden on consumers to become better and more informed purchasers of health services. In today's healthcare system, patients are increasingly asked and expected to become better informed purchasers of health services, but are rarely given the tools needed to do so.[20] HDHPs, or consumer driven health plans, shift financial risk to the individual as a way to reduce employer costs and encourage beneficiaries to find lower cost, higher

---

[18] California Department of Health Care Services, Medi-Cal Monthly Enrollment Fast Facts, January 2017, available at http://www.dhcs.ca.gov/dataandstats/statistics/Documents/Fast_Facts_January_2017_ADA.pdf.

[19] Andrea Sorensen, Narissa J. Nonzee, and Gerald F. Kominski, Public Funds Account for Over 70 Percent of Health Care Spending in California, 3, available at http://healthpolicy.ucla.edu/publications/Documents/PDF/2016/PublicSharePB_FINAL_8-31-16.pdf.

[20] U.S. Government Accountability Office, "Meaningful Price Information Is Difficult for Consumers to Obtain Prior to Receiving Care." Sept. 23, 2011. Available at http://www.gao.gov/products/GAO-11-791. Martha Hostetter and Sarah Klein, "Health Care Price Transparency: Can It Promote High-Value Care? *Commonwealth Fund*, April/May 2012. Available at http://www.commonwealthfund.org/publications/newsletters/quality-matters/2012/april-may/in-focus.

quality options. In 2006, just 4% of covered workers were enrolled in HDHPs nationally.[21] In 2016, the number of covered employees enrolled in such plans rose to 29%.[22] Consumers are, therefore, increasingly asked and expected to consider the cost and quality of services when making health care decisions. Yet, with price opacity and fragmented quality information, consumers rarely have the easy access to the data required to make such decisions. A recent study funded by the Robert Wood Johnson Foundation and the New York State Health Foundation, for example, found that only 20% of Americans have attempted to compare price information across multiple providers.[23] The primary reasons given by respondents for not comparing prices included a lack of awareness that prices varied across providers and an inability to find price information. The need for price information tools has only grown deeper with the enactment of the ACA and the popularity of HDHPs in the ACA marketplaces.[24]

APCDs can serve as a cost and quality comparison tool for patients and provide the exact information and access that is currently impeding the type of empowered consumer activity that HDHPs demand. APCDs have the potential to make some healthcare services, namely those that patients find readily substitutable for one another, such as blood tests, X-rays, and CT scans, "shopable" by pairing pricing and quality information. For example, Massachusetts mandates the creation of a consumer website to facilitate comparison shopping.[25] Efforts to create price transparency websites for consumers from payer data mirror certain voluntary efforts by large insurers and hospital systems to encourage shopping among their affiliated providers by posting price data directly, or collaborations between the state and hospital associations to do the same. These APCD systems point patients toward better and cheaper providers while also fostering competition between providers.

Finally, data collected, maintained, and disseminated by APCDs can assist consumers, policymakers, state agencies to identify and challenge the increasingly concentrated market power of

---

[21] Gary Claxton, Matthew Rae, Michelle Long, Anthony Damico, Bradley Sawyer, Gregory Foster, Heidi Whitmore, and Lindsey Schapiro, "Employer Health Benefits: 2016 Annual Survey," available at http://www.kff.org/report-section/ehbs-2016-summary-of-findings/.

[22] Gary Claxton, Matthew Rae, Michelle Long, Anthony Damico, Bradley Sawyer, Gregory Foster, Heidi Whitmore, and Lindsey Schapiro, "Employer Health Benefits: 2016 Annual Survey," available at http://www.kff.org/report-section/ehbs-2016-summary-of-findings/.

[23] David Schleifer, Rebecca Silliman, and Chloe Rinehart, Still Searching: How People Find and Use Health Care Price Information in the United States, available at https://www.publicagenda.org/files/PublicAgenda_StillSearching_2017.pdf.

[24] Because premium tax credits are pegged to the second-lowest-cost silver plan, for consumer eligible for tax credits, the silver and bronze plans are the most inexpensive options. The average silver and bronze plans are considered HDHPs, with deductibles of $2,500 and $5,2300, respectively.

[25] Center for Health Information and Analysis, Overview of the Massachusetts All Payer Claims Database (March 2014), available at https://www.apcdcouncil.org/sites/apcdcouncil.org/files/media/state/ma-apcd-overview-2014.pdf.

providers. Provider consolidation has been shown to increase prices, particularly in areas like Northern California where concentration is already high. For instance, studies have shown that a merger between closely competing hospitals can cause healthcare prices to rise by 20-60%. [26] Consolidation and the associated reductions in competition not only threaten the healthcare system through higher prices, but provider concentration and decreased competition risks quality reductions—particularly in administered pricing systems like Medicare.[27] The availability of healthcare claims data, particularly the availability of transparent pricing information, can provide a useful check on the ill effects of consolidation. The data provided by an APCD can empower state agencies' efforts to monitor and analyze the quality and cost effects of hospital consolidation across the state, allowing agencies to identify problem markets and properly employ regulatory tools to address the negative effects of overly concentrated markets.[28]

Balancing Access and Privacy

APCDs provide important tools in the struggle to control health care costs and improve quality. However, policymakers, health care advocates, and consumers must balance the many benefits that APCDs offer against the need to protect patient privacy and data security. To be an effective resource for control costs and quality improvement, APCDs must be able disclose collected information to government agencies, providers, insurers, and researchers, while carefully protecting individuals' personal and sensitive data. The APCD must ensure the privacy and security of the data during the collection, storage, disclosure, and use of the data.

II. California

Beginning in 2014, the Senate Health Committee held discussions with health care experts aimed at understanding and addressing the rising costs of health care in California.[29] One potential

---

[26] Martin Gaynor, "Hew Health Care Symposium: Consolidation And Competition in US Health Care." *Health Affairs Blog*, March 1, 2016, available at http://healthaffairs.org/blog/2016/03/01/new-health-care-symposium-consolidation-and-competition-in-us-health-care/.

[27] Martin Gaynor and Robert Town, "The impact of hospital consolidation—Update." The Robert Wood Johnson Foundation, June 2012, available at http://www.rwjf.org/content/dam/farm/reports/issue_briefs/2012/rwjf73261.

[28] While the effects of ERISA preemption on states' ability to compel self-insured employers to submit health claims data to APCDs will limit the utility of a state APCD's data and the generalizability of research obtained from that data, access to even a limited dataset is infinitely preferable to the status quo. A more complete discussion of ERISA preemption and its effects on APCDs and state health policy reform efforts is outside the scope of this report, but more information can be found at Erin C. Fuse Brown and Trish Riley, Empowering and Protecting Consumers: ERISA Thwarts State Innovation, available at http://nashp.org/empowering-and-protecting-consumers-erisa-thwarts-state-innovation/.

[29] Assembly Committee on Privacy and Consumer Protection, June 28, 2016, p. 4.

policy solution that emerged from these discussions was the creation of a comprehensive database of state-wide cost and quality information. According to the proponents of such a database, a comprehensive cost and quality data would promote the goals of providing efficient, affordable, and equitable health care services to all Californians.[30] Despite the potential value of access to APCD data for consumers and policy makers, consumer advocacy groups in California, led by the American Civil Liberties Union (ACLU) and the Consumer Federation of California (CFC), recently opposed SB 1159—a bill that would have created the California Health Care Cost and Quality Database. The opposition from the ACLU and CFC arose due to concerns that the proposed legislation did not sufficiently protect private health information.

Senate Bill 1159

The intent of SB 1159 was to establish the California Health Care Cost and Quality Database (the "Database"). SB 1159 aimed to create a comprehensive repository of health care cost and quality information that can be used by consumers, payers, providers, and government entities to improve health care purchasing and lower costs, increase efficiency, and encourage policy innovations.

In the initial version of legislation proposing the creation of the Database, SB 1159 directed the Secretary of CHHS to convene an advisory committee composed of a "broad spectrum" of health care stakeholders. The membership was to include all entities that were required by SB 1159 to submit information to the Database—health care services plans, insurers, suppliers, providers, self-insured employers, and multiemployer self-insured plans—as well as representation from various health care purchasers. The representation of purchasers on the advisory committee was to include business, organized labor, and consumer representatives. The Secretary was also free to appoint additional purchaser representatives to the committee.

SB 1159 directed the advisory committee to provide consultation regarding the types of data to be collected by the APCD, the purposes to which the data was to be used, and the entities and individuals that should be required to report to and have access to the Database. As established by SB 1159, the governance structure and oversight body shared many similarities with the other states reviewed below. The key similarities include the broad representation of providers, payers, purchasers, and consumers, as well as the general responsibilities for advising the Database administrators on the collection of and access to health data.

SB 1159 was, however, notable for the absence of robust privacy and security provisions. While SB 1159 did contain language requiring all uses and disclosures of data *comply* with applicable state and federal data privacy laws, including direct references to the Confidentiality of Medical Information Act (CMIA), the Information Practices Act (IPA), and the federal Health Insurance Portability and Accountability Act (HIPAA), such language did not, in fact, subject the Database to any meaningful privacy or security requirements. Under both HIPAA and CMIA, a government entity is not considered a "covered entity," and is not, therefore, subject to the data security or privacy requirements established

[30] Assembly Committee on Privacy and Consumer Protection, June 28, 2016, p. 4.

by either law. As such, despite language in SB 1159 requiring "compliance" with HIPAA and CMIA, the security and privacy protections established by these laws would not be enforceable upon the Database or the California Health and Human Services Agency (CHHSA).

The Database would have, however, been governed by California's Information Privacy Act (IPA). The IPA applies specifically to the disclosure of personal information by government actors and entities. All three laws, HIPAA, CMIA, and the IPA, establish broad prohibitions against the disclosure of personal health information without prior authorization, but the IPA provides overly broad exceptions to the general prohibition. Of primary concern is language within the IPA that allows for the disclosure of personal information when the information is necessary for a government entity to "perform its constitutional or statutory duties."[31] The inapplicability of CMIA and HIPAA to the Database and the overly broad exceptions established by the IPA were the primary points of concern with the initial drafting of SB 1159.

Additional privacy and security concerns also arose from language in SB 1159 that prohibited the "public" disclosure of unaggregated, individually identifiable health information. The CFC raised objections stemming from the absence of any prohibition against the "private" disclosure of unaggregated, individually identifiable health information.[32] CFC believed that the absence of such language regarding private disclosures implied that there was, in fact, no limit on such disclosures. The privacy and security concerns of both the ACLU and CFC led them to propose amendments to SB 1159 that, instead of requiring compliance with HIPAA and CMIA, would make the Database subject to CMIA and HIPAA. The addition of such an amendment would make HIPAA's and CMIA's security and privacy and protections enforceable upon the Database, as though it were a covered entity. As a result of the pressure exerted by the ACLU and CFC, an author's amendment was added to make CHSSA, and therefore the Database, subject to CMIA and HIPAA.[33] Had SB 1159 proceeded in this amended form, the enacting legislation of the California Database would have closely resembled its Colorado counterpart in regards to the enforceability of HIPAA to the Database.

Despite the addition of amendments that would have subjected the Database to both HIPAA and CMIA, legislators also amended SB 1159 to alter its intent from *establishing* the Database to *researching* options for developing the California Health Care Cost, Quality, and Equity Data Atlas.[34]

---

[31] Assembly Committee on Privacy and Consumer Protection, June 28, 2016, p. 6.

[32] Assembly Committee on Health, June 21, 2016, p. 7.

[33] Assembly Committee on Privacy and Consumer Protection, June 28, 2016, p. 6.

[34] The altered intent of SB 1159 is first reflected in the amended Assembly version from August 15, 2016.

Existing Privacy Protections and their Applicability to a California APCD

Developing the California Health Care Cost, Quality, and Equity Data Atlas ("the Atlas") requires an understanding of the current federal and state laws that protect personal health information, and whether and how those laws can apply to data transmitted to and disclosed from the Atlas. This Report examines the federal Health Insurance Portability and Accountability Act, and California's Confidentiality of Medical Information Act and the Information Practices Act for their potential applicability to the Atlas.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The HIPAA "Privacy Rule" was issued by the Department of Health and Human Services in 2000 and became effective in 2001.[35] The Privacy Rule established a national standard for the protection of health information. The national standard established by HIPAA acts as the national "floor" for protecting the use and disclosure of health information. HIPAA preempts state laws that are contrary and less protective, but states are free to maintain existing laws or enact new laws that are more stringent. Most pertinent to the development and operation of an ACPD, HIPAA established strict procedures and requirements for data release and data security, but those restrictions only apply to covered entities.

HIPAA's Privacy Rule applies to three types of "covered entities": health plans, health clearinghouses, and providers who transmit information in electronic form. A health plan as defined by HIPAA includes government and private plans, individual and group plans, as well as employer-sponsored benefit plans. HIPAA defines a "clearinghouse" as an entity that receives health information from a covered entity and translates it into or from a standard format. In the absence of legislative language requiring otherwise, entities that fall outside the definition of "covered entity" are not, therefore, subject to HIPAA's security and privacy provisions. As a result, government entities, including government-run APCDs, are not covered entities under HIPAA. Therefore, legislative language that required the Atlas to "comply" with HIPAA would not, in fact, place any meaningful requirements on the Atlas or its employees. In order to make HIPAA's Privacy Rule apply to the Atlas, the legislation must include language making it "subject to" HIPAA's requirements for covered entities, rather than requiring "compliance" with HIPAA.

"Health information," as defined by HIPAA, includes past, present, or future physical or mental health conditions, the provision of health care to an individual, or past, present, or future payment for the provision of health care. Such information is considered "protected health information," or "PHI," if it is individually identifiable and if it is transmitted or held by a covered entity, regardless of the medium

[35] Compliance was generally required by 2003.

(oral, paper, or electronic).[36] HIPAA does not place any restrictions on the use or disclosure of de-identified health information by covered entities, but does provide useful guidance on the process by which health information is de-identified.[37]

The HIPAA Privacy Rule prohibits the use or disclosure of PHI by a covered entity without the written authorization of the individual. HIPAA does, however, permit the use and disclosure of PHI without prior authorization under certain limited circumstances.[38] For the purposes of understanding the legality of uses and disclosures of PHI as it relates to the establishment and operation of an APCD, two exceptions are of primary relevance. The first exception applies to PHI uses or disclosures required by law.[39] Under the HIPAA Privacy Rule, when a law, including a statute, regulation, or court order, requires the use or disclosure of protected health information by a covered entity, that covered entity may disclose the protected information without the authorization of the individual. The second exception permits the use and disclosure of protected health information for research purposes under certain circumstances.[40] Under the HIPAA Privacy Rule, "research" is defined as the "systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[41] HIPAA does not, however, create a blanket exception for research purposes, but rather establishes a limited set of circumstances and procedures through which a covered entity may use or disclose PHI for research purposes without prior written authorization.[42] In addition, for nearly all uses and disclosures of PHI made by covered entities, the disclosure must be limited to the "minimum necessary" needed to achieve the stated goal of the use or disclosure.

In addition to the requirements and restrictions regarding the use and disclosure of PHI by covered entities, HIPAA also establishes a series of security procedures and responsibilities that covered entities must follow that the legislature could apply to the Atlas. All covered entities must ensure the confidentiality, integrity, and availability of electronic PHI that they create, receive, maintain, or transmit.[43] HIPAA also requires covered entities to establish protections against any "reasonably

---

[36] Individually identifiable is defined to include both when the identity of the individual can be directly known or if there is a reasonable basis to believe the identity can be determined.

[37] See 45 C.F.R. § 164.514(b)(2017).

[38] See 45 CFR §164.512 (a-l) (2017).

[39] 45 CFR §164.512(a)(2017).

[40] 45 CFR §164.512(i) (2017). Research is defined by HIPAA to mean the "systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge" (see 45 CFR 164.501)(2017).

[41] 45 CFR §164.501(2017).

[42] 45 CFR §164.512(i) (2017).

[43] 45 CFR §164.306(a)(1)(2017).

anticipated threats or hazards" to the security of electronic PHI.[44] In recognition of the ever-changing data security environment, HIPAA requires covered entities to review and modify their security procedures in order to ensure that the procedures remain "reasonable and appropriate" over time.[45] HIPAA also requires covered entities to establish procedures to "prevent, detect, contain, and correct" security violations, as well as put in place policies to assess the risk and vulnerability of the confidentiality and integrity of the electronic PHI maintained by the covered entity.[46] In the case of a data breach, HIPAA generally requires the covered entity notify the individuals whose PHI was, or is reasonably believed to have been, accessed as a result of the breach.[47] In addition to the above-described privacy and security procedures, HIPAA includes additional requirements concerning physical and technical safeguards for PHI,[48] as well as requirements for the training of a covered entity's personnel to appropriately and securely work with PHI.[49]

The Confidentiality of Medical Information Act (CMIA)

The Confidentiality of Medical Information Act (CMIA) was enacted by the California legislature in 1981 as Cal. Civ. Code §§ 56-56.37. Similar to HIPAA, CMIA establishes a broad prohibition against the disclosure of medical information without the prior authorization of the individual whose data is concerned. The rules and regulations established by CMIA govern the use and disclosure of medical information by providers, employers, and third-party administrators. CMIA, like HIPAA, does not, therefore, apply to government entities. Therefore, as was true with applicability of HIPAA to an APCD, in the absence of legislative language specifically subjecting the Atlas to CMIA, it would not be compelled to follow CMIA's privacy and security procedures.

Should the California legislature subject the Atlas to CMIA, the most pertinent sections of CMIA to its development and operation are Sections 56.10 and 56.101. Section 56.10 establishes the exceptions under which a health plan or provider may disclose medical information without prior authorization. Similar to HIPAA, CMIA permits the disclosure of medical information without prior authorization for "bona fide research purposes" and when the disclosure is authorized by law.[50] In addition to the restrictions on the disclosure of medical information, CMIA also imposes strict prohibitions against the re-disclosure of any medical information that was initially disclosed pursuant to

---

[44] 45 CFR §164.306(a)(2)(2017).

[45] 45 CFR §164.306(e).

[46] 45 CFR §164.308.

[47] 45 CFR §164.404.

[48] 45 CFR §164.310; 45 CFR §164.312.

[49] 45 CFR §164.530.

[50] Cal. Civ. Code §56.10(c)(7); §56.10(c)(14).

CMIA.[51] As such, if the California legislature specifically subjected the APCD to CMIA, it would operate as a covered entity under CMIA, thereby limiting both disclosures from the APCD and re-disclosures from entities receiving the information from the APCD.

In addition to establishing state-level requirements for the protection and disclosure of medical information, CMIA offers the most general of data security requirements. Section 56.101 establishes the broadly worded security requirement that all providers, health care service plans, pharmaceutical companies, or contractors "preserve" the confidentiality of medical information when creating, maintaining, preserving, storing, abandoning, destroying, or disposing of medical information. An important omission from the activities covered by this provision is the "disclosure" of medical information. HIPAA, therefore, operates to set a higher security "floor" for the security of protected health information than CMIA.

The Information Practices Act

Enacted in 1977, the Information Practices Act (IPA) would also apply to the Atlas, as it specifically governs the disclosure of personal information by California government agencies.[52] In its definition of "personal information," the IPA specifically includes a person's medical history, as well as the sensitive demographic data commonly included in medical claims data.[53] Furthermore, the IPA defines "agency" to include "every state office, officer, department, division, bureau, board, commission, or other state agency."[54] Therefore, under the IPA's definition of "personal information" and "agency," the IPA would govern any disclosure of personal information from the Atlas. In fact, the applicability of IPA to information collected by the Database pursuant to SB 1159 proved sufficient to convince the California Senate Judiciary Committee to dismiss concerns by the ACLU that CMIA and HIPAA would not apply to the Database.[55]

The IPA prohibits government agencies from disclosing personal information in any manner that could link the information to the individual. The IPA does, however, provide a limited set of circumstances in which a government entity can disclose identifiable information. Similar to both HIPAA

---

[51] Cal. Civ. Code §56.13.

[52] Cal. Civ. Code §§ 1798-1798.78.

[53] "Personal information" is defined by the IPA to mean "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual" (1798.3(a)).

[54] The term "agency" as used in the IPA does not, however, include, the California Legislature, any agency established under Article VI of the California Constitution, the State Compensation Insurance Fund, except as to any records which contain personal information about the employees of the State Compensation Insurance Fund, or a local agency, as defined in subdivision (a) of Section 6252 of the Government Code (see 1798.3(b)(1-4).

[55] Senate Judiciary Committee Hearing, April 19, 2016, p. 7.

and CMIA, the IPA also includes exceptions for the disclosure of personal information when required by law and for research purposes. When required by state or federal law, the IPA permits the disclosure of personal information to a government agency. Unlike HIPAA and CMIA, this exception allows only for the disclosure of personal information to a government agency.[56] Neither HIPAA nor CMIA narrows the allowable recipients to such an extent. Similar to HIPAA and CMIA, however, the IPA allows for the disclosure of personal information without prior authorization for the purposes of statistical research. [57] Even under such circumstances, however, the IPA specifies that the data cannot be identifiable. The IPA also contains an additional research-specific exception that applies to the disclosure of personal information to the University of California.[58] The University of California-specific exception does not restrict the disclosure to only de-identified data. It does, however, establish additional requirements that researchers must satisfy prior to the disclosure of data under this provision.[59] Additionally, the IPA permits the disclosure of personal information without prior authorization when the disclosure is necessary for the transferee agency to "perform its constitutional or statutory duties."[60] This "constitutional or statutory" exception concerned the ACLU and CFC most and led them to ask the legislature to subject the Database to CMIA and HIPAA.

In addition to establishing rules and requirements governing the release of personal information by government entities, the IPA also creates security requirements applicable to an APCD. Under the IPA, an agency must establish rules of conduct for personnel involved in the design, development, operation, disclosure, or maintenance of personal information.[61] An agency must also erect "appropriate and reasonable" administrative, technical, and physical safeguards to protect the security and confidentiality of records containing personal information.[62] The agency must also take steps to protect personal information from anticipated threats or hazards that could "result in any injury." HIPAA includes similar security procedures and language. The IPA, therefore, provides an existing state-level mechanism to establish security measures that are equal to or more stringent than those created by HIPAA.

The existing privacy and security provisions provided in HIPAA, CMIA, and IPA all provide guidance on both what existing law requires and what the California legislature could easily require of the Atlas to protect personal and de-identified health information.

---

[56] Cal. Civ. Code § 1798.24(f).

[57] Cal. Civ. Code § 1798.24(h).

[58] Cal. Civ. Code § 1798.24(t)(1).

[59] Cal. Civ. Code § 1798.24(t)(1)(A-E).

[60] Cal. Civ. Code § 1798.24(e).

[61] Cal. Civ. Code § 1798.20.

[62] Cal. Civ. Code § 1798.21.

III. Guidance from Existing State APCDs

In addition to the privacy laws applicable in California, this Report analyzes four state APCDs to gauge the variety of state privacy and security procedures. It examines the structure and policy of existing APCDs in Maine, Massachusetts, and Colorado, as well as the development of the New York APCD. We selected these four states based on a variety of factors:

- **Maine** established the first APCD - The Maine Health Data Organization (MDHO) – in 1996 and has collected insurance claims data since 2003.[63]

- **Massachusetts** has nearly universal health coverage and its APCD has a unique relationship to the Massachusetts Health Policy Commission (HPC), an independent state agency charged with analyzing health care data within the state to lower costs and improve quality.

- **Colorado** has a robust and patient-centered APCD dedicated to providing consumers and researchers with relevant healthcare price information.

- **New York** is in the process of developing its APCD almost entirely under the guidance of the Commissioner of Public Health in consultation with the Public Health and Health Planning Commission (PHHPC), rather than by statute, which provides an interesting legislative model.

After reviewing the implementing legislation and regulations for each APCD, we defined three areas as key to establishing sound privacy and security procedures - the governance structures and oversight procedures, the security measures, and the disclosure requirements and processes. Policy choices in each of these three areas determine how states balance the utility of access to APCD-housed information and protection of private health information. This section analyzes the policies and procedures established in each of these areas and compares and contrasts practices across the four states.

Governance Structures and Oversight Institutions

The design of an APCD's governance structure and oversight capacity can promote transparency and accountability, while also extending the administrative and operational capabilities of the ACPD. The state APCDs vary on several factors related to governance structure and oversight capacity: the permanence of the oversight bodies, the oversight bodies' membership, and the governance and operational responsibilities given to the oversight body. States can design these structures in ways that promote continued enhancement of data protection and security measures within the APCD.

---

[63] Maine Health Data Organization, Claims – The All Payer Claims Database, available at: https://mhdo.maine.gov/claims.htm.

Maine

Maine's MDHO is an independent executive agency tasked with creating and maintaining a "useful, objective, reliable, and comprehensive health information database" to improve the health of Maine citizens and issue reports on the health care system.[64] The MHDO operates under the guidance and supervision of a board of directors. The board has 20 voting members and 1 non-voting member. Maine cedes the vast responsibility for appointing members to the agency to the governor. The governor appoints 18 voting members of the board, including 4 members who represent consumers, 3 who represent employers, 2 who represent third party payers, and 9 who represent providers in designated areas such as hospitals, physicians, and federally qualified health centers.[65] The Commissioner of Health and Human Services can appoint one employee of the department as a voting member to represent the State's interest in maintaining health data and to ensure that the stored information is available to guide public health policy. Finally, the Commissioner of Professional and Financial Regulation can appoint one employee of the Department of Professional and Financial Regulation as a non-voting member.

The board has broad authority to develop and implement policies and procedures for the "collection, processing, storage, and analysis of clinical, financial, quality, and restructuring" health care claims data.[66] The Board has full authority to create the rules and regulations governing the operation of the MHDO, release of information, and enforcement and penalties for noncompliance or misuse of data.[67] The MHDO Executive Director and Data Release Subcommittee have the authority to deny any request for data, and such decisions are not reviewable outside the MHDO.

The legislature gave the board the power to contract with one or more nongovernmental, independent third parties, including University of Maine, for data collection, processing, and storage.[68] Furthermore, the legislature granted the board the ability to enter into "all other contracts necessary or proper to carry out [its] powers and duties," which specifically included allowing organization staff to provide technical support or assistance to public or private entities.[69] This broad authority does not limit the entities with whom the board may contract for specific services, as Massachusetts and Colorado have done.

---

[64] 22 22 Me. Rev. Stat. §8703(2017).

[65] 22 Me. Rev. Stat. §8703(2) (2017).

[66] 22 Me. Rev. Stat. §8704(1)(2017).

[67] 22 Me. Rev. Stat. §8704(4)(2017).

[68] 22 Me. Rev. Stat. §8704(2)(2017).

[69] 22 Me. Rev. Stat. §8704(3)(2017).

Massachusetts

In Massachusetts, APCD legislation created the Health Information and Analysis Oversight Council.[70] The Council provides operational capacity and expertise across nearly all aspects of the APCD's activities. The specific responsibilities of the Council, as set forth by law, include preparation of the annual budget, administration of expenses, the development of research and analysis priorities, as well as the establishment of guidelines for the collection, storage, and maintenance of APCD data. The delineation of clear responsibilities is just one factor contributing to the establishment of an effective oversight body. The membership of an oversight body must include the expertise required to fulfill its responsibilities. Like Maine, Massachusetts benefits from an oversight body with a membership that draws from a diverse set of stakeholders. However, Massachusetts goes beyond inclusion of various stakeholders to require that some members have expertise in particular fields, such as academic researcher, health care systems, and cyber-security experts.[71] Requiring expertise on governing boards can promote data security, research use and applicability, and transparency, while providing all potentially affected groups a voice in the APCD's activities.

Of the states reviewed here, Massachusetts is unique in both the manner in which it appoints members of the council and in the specificity with which required expertise is outlined. The Massachusetts APCD legislation specifies that the membership of the Health Information and Analysis Oversight Council include the Secretaries of Health and Human Services and Administration and Finance, as well as the Commissioner of Insurance and the Executive Director of the Health Policy Commission. The inclusion of high-ranking government officials with expertise and authority over health care, insurance, and administration and finance reflects the broad responsibilities given to the Council. In addition to these government officials, the legislation also requires two members of the council be appointed by the Attorney General, two by the state auditor, and three by the governor. Appointment power is not, therefore, concentrated in one person or office, but is diversified across government entities. In order to guarantee the presence of appropriate knowledge and operational capacity, the legislation further requires that one of the Attorney General's appointees have experience in cyber-security, that one of the state auditor's appointees be a health economist, and that among the three members appointed by the governor, one must have experience in health care delivery or management, one must have experience in big data or data analytics, and the other must have experience in finance and budgeting. The legislatively determined appointment process and expertise requirements provide robust oversight of all aspects of the APCD's activities and ensure a broad representation of ideas and voices. Notably, however, Massachusetts did not include a requirement that the Oversight Council include a consumer privacy advocate.

Unlike Maine, the Massachusetts APCD legislation does not permit the contracting of any APCD activities or responsibilities to a third-party—whether to a government agency, non-profit, or for profit

---

[70] M.G.L c. 12 Section 2A(a).

[71] See Mass. Gen. Laws. c.12 §2A(2017).

entity. However, Massachusetts has the Health Policy Commission and other governmental entities that are charged with analyzing the health care data generated by the state. The Massachusetts legislature stated that the restrictions on contracting were imposed to help ensure the privacy of APCD data.

Colorado

Colorado's APCD is led by an Executive Director and an Advisory Council. The Colorado advisory council is responsible for providing recommendations to the executive director and administrator of the APCD on procedures for the collection, retention, use, and disclosure of data. Specifically, the legislation charges the advisory council with recommending procedures for protecting data privacy, integrity, and confidentiality, including procedures for ensuring compliance with HIPAA. The legislation does, however, create uncertainty regarding the strength, impact, and boundaries of the council's recommendations.[72]

The legislation is silent on whether the advisory council's recommendations bind the executive director or whether the executive director retains ultimate decision-making power on all covered issues. The silence of the legislation on the binding or non-binding nature of recommendations leads to the assumption that the recommendations are not binding. In different provisions within section two of the Colorado legislation, the advisory committee is first charged with "overseeing" the APCD and then later with making "recommendations" on a specific universe of APCD activities.[73] The responsibility for "overseeing" seemingly creates a broad authority for the advisory committee, but one that is soon constrained to making recommendations. Additional confusion regarding the boundaries of the advisory council's responsibilities and authority arises from conflicting legislative provisions concerning the relationship between executive director and advisory council in setting operational procedures. Section 5(a), for example, gives the administrator responsibility for determining what data is to be collected and by what method. Yet, section 6(c) states that the determination of what data is to be collected, in what format it is to be collected, and how it will be delivered is to be made by the executive director with the input of the advisory council.

While the legislature left the specific authority of advisory council somewhat uncertain, it was quite clear on the diversity of its membership. The Colorado APCD legislation requires the appointment of an even more diverse advisory committee than that of Massachusetts. In addition to a contingent of government officials (or their designees), the Colorado legislation goes well beyond the requirements of the Massachusetts legislation to include the appointment of consumer representatives, as well as representatives from across the provider and insurance communities, large and small employers, and a member from academia with expertise in health care data and cost efficiency research. The Colorado legislation also obligates the executive director to appoint two members from the State General

---

[72] COLO. REV. STAT § 25.5-1-204 § 2(a-b) (2017).

[73] COLO. REV. STAT § 25.5-1-204 § 2(a-b)(2017).

Assembly. There is, however, no requirement to include a cyber-security expert, a health economist, or a member with expertise in data analytics and/or big data, as was true in Massachusetts. Such expertise may be found among the appointees of the Colorado advisory committee, but the expert criteria delineated by the Colorado legislation is less specific than that of Massachusetts. As a result, the Colorado advisory committee includes a more diverse representation of stakeholders and advocates, but also potentially contains less expertise on the operational specifics of the APCD than Massachusetts, particularly in the area of cyber-security and data privacy.

In addition, the Colorado legislation, unlike that in Massachusetts, places the appointment power for the Colorado advisory committee solely in the hands of the executive director of the Colorado APCD. The absence of shared appointment power in Colorado may, however, be balanced by the legislatively ordered appointment of a wider array of health care stakeholders compared to Massachusetts.

The Colorado legislation allows the administrator, in consultation with the advisory committee, to contract with a third-party for the collection and processing of APCD data. The contracting provisions specifically prohibit the collection of unencrypted social security numbers by a third-party and prohibit the data collected by the third-party from being used for any purpose other than that specified in the contract. The contracting provisions in the Colorado legislation are more liberal than Massachusetts—which does not allow any outside contracting—but Colorado does tightly constrain the activities a third-party can perform.

New York

Unlike Maine, Massachusetts and Colorado, the New York APCD legislation does not establish a permanent advisory or oversight council that is unique to the APCD. Rather, the New York legislation specifies that the Commissioner of Public Health in consultation with the Public Health and Health Planning Commission (PHHPC) will develop and operate the APCD.[74] The PHHPC is an existing advisory body with broad responsibilities over the New York public health and health care systems. The membership of the PHHPC is a diverse collection of health care stakeholders, but unlike other state legislation reviewed here, the New York legislation does not have language that requires the creation of an advisory council specific to the APCD or the appointment of persons with expertise or knowledge specific to the operations of an APCD. The broad membership of the PHHPC, which includes representatives from academic medical institutions, various provider groups, and health policy experts, may contain expertise relating to the development and operation of an APCD, but this structure does not guarantee that membership includes, for example, data privacy and security experts.

In addition to the language relating to the consultative role of the PHHPC, the New York legislation does require that the Commissioner develop regulations in consultation with the superintendent of financial services, as well as health care providers, third-party health care payers, and patient advocates. Unlike the other legislation reviewed here, the New York legislative language does

[74] N.Y. Public Health Law (PHL) § 2816 (1)(a)(2017).

not establish a permanent advisory body or provide further specificity on the number or nature of actors the Commissioner must consult. Also absent from the New York legislation is any requirement to include privacy and security experts, consumer advocates, or representatives from academia. In the absence of a permanent role and the inclusion of such representatives, the New York legislation establishes an advisory body with the most minimally defined role and authority of any legislation reviewed here. In addition to establishing the most limited oversight body, the New York legislation grants the commissioner the broadest authority of any APCD to contract out the operation of the APCD. Similar to Maine, the New York legislation gives the commissioner the authority to contract with any entity it chooses, but it also allows the commissioner to contract with one or more entities to operate *any* part of the ACPD. In Massachusetts, contracting is strictly forbidden and in Colorado, contracting is limited only to the collection of APCD data.

Recommendations

With respect to APCD governance structure and oversight institutions, we recommend the creation of an independent, permanent oversight body with a broad-based membership that requires both representation from specific stakeholder groups, including patient advocates, provider organizations, payers, small and large employers, members of the state legislature, and advocates for protection of individual data on the internet, as well as individuals with expertise critical to the operation of an APCD, including data privacy and security experts, academic researchers, and health economists. We also recommend shared appointment power, as Massachusetts has done, with various entities possessing the ability to appoint members to the oversight body. Finally, the state legislature should provide some restrictions on which entities the oversight body can contract with and ensure those entities are subject to the relevant data privacy laws and protections. If California allows the oversight body to contract with any type of entity, we recommend requiring each contracting entity provide ongoing proof that it has significant data privacy and security measures in place for the duration of the contract. Finally, the governance structure and oversight procedures would also benefit from the inclusion of clear legislative language regarding the binding or non-binding nature of any recommendations issued by the advisor committee.

Privacy and Security Protections

Data collected, stored, and maintained by an APCD is highly sensitive and personal, requiring strong protections against breach and theft. Concerns regarding the centralization of such data within a single entity, particularly given the prevalence of cyber-attacks and the recent targeting of health care

systems and hospitals, are both understandable and reasonable.[75] The four states took significant measures to ensure the security and confidentiality of claims data submitted to an APCD.

Maine

The MHDO board of directors has the power to establish rules and regulations governing the release of information from the MHDO, within the parameters set by the enacting legislation. The legislature aimed to strike the balance between the public utility of claims data and individual privacy by requiring the MHDO to offer public access to non-privileged and non-confidential information, provide a notice and comment period for the public to respond to determinations of whether certain information is privileged or confidential, and then establish rules for allowing disclosure of confidential/privileged information under certain circumstances. As a baseline, the legislature deemed all data collected by the organization that contains protected health information confidential.[76] Such information is not open for public inspection, does not constitute public records, and may not be examined in any judicial, executive, legislative, administrative, or other proceeding as to the existence or content of any individual's identifying health information, except to prosecute civil and criminal violations regarding information in the organization database.[77]

The Maine legislature also specified that the board should establish rules for the release of data at three levels: 1) de-identified data; 2) limited data sets; and 3) protected health information (confidential/privileged information). All releases must be governed by a data use agreements (DUAs) that provide adequate privacy and security measures for the specified level of data, including appropriate accountability and notification requirements.[78] A blank DUA form with all the requirements is easily accessible on the MHDO webpage. The legislature also required the board to establish a Data Release Subcommittee to review and adjudicate Level III data requests.

While the MHDO Board did not make HIPAA's provisions for release of protected health information directly apply to MHDO data releases, it did incorporate much of the language and concepts from the federal law into Level III data release protocols. For instance, MHDO can release Level III data to "covered entities and their business associates," for the purposes of treatment, payment, and health

---

[75] Nicole Perlroth and David E. Sanger, "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool." *New York Times*, May 12, 2017. April Glaser, "U.S. hospitals have been hit by the global ransomware attack." *Recode*, June 27, 2017.

[76] 22 Me. Rev. Stat. §8714(1)(2017).

[77] Id.

[78] 22 Me. Rev. Stat. §8714(3)(2017).

care operations, directly incorporating HIPAA's definitions for those terms into the MHDO regulations.[79] These references to HIPAA grant the MHDO both credibility in setting its floor, and flexibility to expand beyond HIPAAs requirements.

The MHDO board also established regulations to enable an individual to refuse to permit the MHDO to disclose and use the individual's identifiable health information in Level III data releases.[80] Allowing individuals the ability to opt out of having their identifiable health information released for any reason provides an important protection for all patients.

Finally, the MHDO has a very robust set of data security and privacy policies. The MHDO adheres to the security and privacy policies established by the State's Office of Technology (OIT) and requires, amongst other things, a security and privacy officer to identify and analyze potential risks, annual assessment of security policies and procedures, and substantial workforce training and guidance.[81]

Massachusetts

Unlike Maine, the Massachusetts legislation does not establish privacy and security protections that are unique to the APCD itself. The legislation specifies that all data-sharing by the APCD is subject to applicable state and federal laws, but does not directly address the APCD's collection and storage of data.[82] CHIA is, however, governed by the Fair Information Practices Act (FIPA)—a Massachusetts law that applies to "every holder maintaining personal data."[83] Among its provisions, FIPA requires all holders of personal data to take all reasonable precautions to protect data from identity theft, theft, and various other physical threats, including fire, flood, and natural disaster. While the Massachusetts legislation only requires data-sharing to be subject to state and federal law, FIPA's "reasonable precautions" appear to apply to data-sharing as well as storage of personal data.[84] Because CHIA is a government entity, it is not considered a "covered entity" under HIPAA, and, therefore, is not subject to HIPAA's security and privacy protections.

---

[79] 90-590-120 ME. CODE R. § 2(5) and (9)(2017) (defining business associate and covered entity); 90-590-120 ME. CODE R. § 8(2)(B) (2017) (permitting the release of identifiable data to covered entities that are data providers and covered entities' business associates for the purpose of treatment, payment, or healthcare operations).

[80] 90-590-120 ME. CODE R. § 13(1)(A)(2017).

[81] 90-590-120 ME. CODE R. § 15(2017).

[82] Mass. Gen. Laws. c.12 § 12 (2017).

[83] Mass. Gen. Laws. c. 66A(2017).

[84] FIPA also mandates that where feasible, a record of every access and use by a person or organization must be maintained. This requirement does not extend to the holder of the data. As such, CHIA could access and use the data itself without having to report each access or use.

However, the Massachusetts APCD regulations establish strong security and privacy protections that, in many respects, go beyond HIPAA's requirements. The security measures developed by CHIA to protect the confidentiality and integrity of the APCD data must, according to the enacting legislation, be reported on CHIA's consumer-facing website. Among the security measures described within CHIA's Privacy Program on the CHIA website include masking, encryption, and filters.[85] The reporting requirement extends CHIA's transparency efforts and aligns with the notice and transparency recommendations of the Fair Information Practices Principles.

To further protect patient confidentiality, the Massachusetts legislation prohibits all contracting with third-party entities for the purposes of operating any of CHIA's activities.[86] This prohibition extends to non-profits and other government entities. To this end, Massachusetts' law requires that CHIA be the sole repository for health care data and be solely responsible for the collection, storage, and maintenance of health care data. Within the states reviewed here, the prohibition against all contracting is unique to Massachusetts.

Colorado

The Colorado APCD legislation makes the state's APCD directly subject to the requirements of HIPAA.[87] As noted above, an APCD is typically a government institution, and, therefore, not considered a covered entity under HIPAA and not subject to HIPAA's robust privacy and security regulations. The Colorado legislation, however, unlike the other states reviewed here, includes language that specifically subjects the APCD collection, storage, and release of health care data to HIPAA requirements. By subjecting the Colorado APCD to HIPAA, the APCD is required to ensure the confidentiality and integrity of all personal health information it receives, maintains, or transmits. The APCD is also required to take steps to protect against "any reasonably anticipated" threat or hazard to the security of APCD data. The APCD must also protect against "any reasonably anticipated" unpermitted uses or disclosures.[88] HIPAA also requires the implementation of administrative safeguards to prevent, detect, contain, and correct security violations. When a breach is discovered or personal health information is determined to have been unsecured, an entity subject to HIPAA must notify the individuals whose PHI has been accessed or whose PHI is reasonably believed to have been accessed.[89]

The HIPAA requirements, however, act only as a minimum floor for privacy and security protections for the Colorado APCD. The Colorado legislation provides the APCD administrator authority

---

[85] The Center for Health Information and Analysis, Privacy Program, available at http://www.chiamass.gov/privacy-program/

[86] Mass. Gen. Laws. c.12 § 12(a)(2017).

[87] COLO. REV. STAT § 25.5-1-204 (8) (2017).

[88] 45 C.F.R. § 164.306 (2017).

[89] 45 C.F.R. § 164.404 (2017).

to establish security and privacy protections, as well as data release requirements that exceed the protection levels set by HIPAA. Beyond the requirements of HIPAA, sections two and five of the Colorado legislation gives the administrator and the advisory committee considerable discretion to build additional layers of protections and create more robust data collection, storage, and release procedures. Section 2(b)(I), for example, states only that procedures and safeguards be established to protect data privacy and confidentiality in the collection, retention, and disclosure of data.[90] In establishing privacy and security protections, the Colorado legislation also directly acknowledges the trade-offs between ensuring the security and privacy of data while also maintaining procedures that allow for the data to be shared and analyzed. Section 5(g) directs the administrator to establish procedures that comply with state and federal privacy laws, but that also preserve the ability to analyze and share data.[91] Additional provisions of the enacting legislation require that the administrator file annual reports that include information pertaining to how APCD data was used, for what purpose, and who requested data. Similar to Massachusetts, the reporting requirements contribute to the transparency and openness with which the APCD conducts its data collection, release, and publication.

New York

The New York APD legislation mandates that the commissioner promulgate regulations that protect the confidentiality of patient identifiable information. This broad mandate does not gain any considerable specificity with subsequent provisions of the New York legislation. The legislation only adds the additional requirement that the commissioner assure the protection of patient privacy in data collection, publishing, release, and access.[92] The provision further requires that such standards should comply with applicable federal law. If, however, the New York APD operates as a government entity, HIPAA, which operates as the primary federal law pertaining to personal health information, would not apply. As such, the New York APD could be in "compliance" with HIPAA without having to follow any of HIPAA's requirements. On the other hand, the New York APD legislation grants its commissioner significant flexibility to establish state-of-the-art privacy practices that evolve alongside technology, without being tied to legislation that can be difficult to modify.

Recommendations

We recommend that California follow Colorado's approach and include legislative language that specifically subjects the Atlas to HIPAA and CMIA. As a government entity, an APCD is not considered a "covered entity" under HIPAA or CMIA, and, therefore, would not be required to follow either HIPAA's or CMIA's security and privacy requirements. This approach would establish HIPAA and CMIA as the minimum, "floor" level for security and privacy procedures, but would allow the legislature or the Secretary of CHHSA and the APCD oversight body to establish additional requirements and procedures to supplement the privacy foundations created by HIPAA and CMIA. Further, incorporating well known

---

[90] COLO. REV. STAT § 25.5-1-204 (2)(b)(I) (2017).

[91] COLO. REV. STAT § 25.5-1-204 (5)(g).

[92] N.Y. Public Health Law § 2816(2)(b)(2017).

and understood privacy and security requirements like those included in HIPAA and CMIA provides assurances to patients that their data will be protected by measures they are accustomed to, without requiring the legislature or the oversight body to draft and consistently update an entirely new set of regulations.

Data Release

The release of data that simultaneously allows for the critical analysis of the health care system and ensures data security and patient privacy is the central task of any APCD. To achieve this primary function, those overseeing the APCD must establish a clear and robust set of procedures to govern the collection, maintenance, storage, and release of APCD data. State legislation varies in regards to the restrictions placed on the release of de-identified and identifiable data. Some states specify a particular set of purposes for which data can be released, as well as identify different types of data that can only be requested by certain categories of requestors. Other states, however, have enacted legislation that provides only minimal criteria for the collection, maintenance, storage, and release of data. Such states give considerable discretion and authority to executive directors or administrators to establish privacy and security protections through regulations. Another key structural difference among states that can impact security and privacy is the extent to which legislation allows for the contracting out of APCD activities to a third-party. The variation among states reviewed here ranges from a complete prohibition in Massachusetts to New York's permissive structure that allows the commissioner to contract out *any* APCD activity. In addition to variations in the procedures and protections for data security and privacy, the states also vary significantly in the clarity and specificity with which legislative language addresses these critical APCD functions.

Maine

The MDHO aims to make data publically available and accessible to the broadest extent consistent with the laws protecting individual privacy, and proprietary information.[93] The MHDO's governing regulations state that "the primary use of MDHO Data is to produce meaningful analysis in pursuit of improved health and health care quality for Maine people."[94] The MHDO Board has established significant rules and regulations governing the release of MHDO data to the public.[95]

First, the Board determined that "acceptable uses of MDHO Data include, but are not limited to, study of health care costs, utilization and outcomes; benchmarking; quality analysis; longitudinal research; other research; and administrative or planning purposes."[96] This broad, but not conclusive,

---

[93] 90-590-120 ME. CODE R. § 1(1) (2017).

[94] Id.

[95] 90-590-120 ME. CODE R. § 1(1) (2017). Standard MHDO DUAs are published on the MHDO Public Website.

[96] Id.

definition provides guidance on the appropriate types of uses for MHDO data without overly constraining potential other and future uses.

Second, all APCD data releases in Maine must be governed by a data use agreement (DUA) that establishes the required privacy and security measures, including appropriate accountability and notification requirements.[97] The DUA details the data recipient's commitments to data privacy and security, as well as the restrictions on the disclosure and use of the MHDO data. The restrictions and privacy requirements specified in the DUA vary depending on the level of data release requested. As noted above, the board established three levels of data: 1) de-identified data; 2) limited data sets; and 3) protected health information (confidential/privileged information). The level of data requested governs many of the terms of the release, while some provisions apply to all data releases.[98]

All data, which the MHDO has not made public, must be requested by application via a standardized application form. The application form enquires about a wide range of factors, including: the individual or entity requesting the data, the level of data requested, how the applicant will use the data, whether an Institutional Review Board (IRB) will oversee use of the data, the ultimate recipient or user of the data, and the security and privacy measures that the applicant will take to ensure patient privacy.[99] The MHDO will only grant access to the minimum amount of data necessary for an approved purpose, and applicants requesting Level II or Level III data must describe how the data requested meets the standard of "minimum necessary."[100]

Level III data can be released on a very limited basis. In line with HIPAA, the MHDO can release Level III data on a limited basis to covered entities that are data providers and their business associates for treatment, payment, and health care operations purposes, provided the MHDO permits the use and the data recipients are bound by the MHDO data use agreement.[101] Level III data may also be used for Health Care Improvement Studies, but only involving patients with whom the study entity has a treatment or payer relationship.[102]

---

[97] Maine requires the same level of appropriate accountability and notification requirements as required of business associates under HIPAA. 22 ME. REV. STAT. §8714(3)(2017).

[98] 90-590-120 ME. CODE R. § 3(3)(2017).

[99] 90-590-120 ME. CODE R. § 3(2)(2017).

[100] Id.

[101] 90-590-120 ME. CODE R. § 8(2)(D) (2017).

[102] 90-590-120 ME. CODE R. § 8(2)(C)(2017).

Some data may not be released at all. For instance, any data that indirectly identifies or would lead to the indirect identification of providers performing abortions[103] or information indicating an individual's HIV status, psychiatric treatment history or substance abuse treatment history may not be released.[104] With respect to payments, the MDHO may not release data related to health care facility or practitioner charges, including total charges, line item charges, or the charge amount for services rendered, unless they are averaged or aggregated in a way which prevents a charge/paid ratio from being computed for each type of service rendered for any individual claims processor, facility, or practitioner.[105] Information on payment of claims is, however, publically available following MHDO approval.

MHDO requires all data recipients to demonstrate levels of security and privacy practices that are commensurate with health industry standards for PHI, and encrypt data both at rest and in transit. Data recipients must be able to demonstrate their ability to meet privacy and security requirements prior to data release.

Interestingly, in 2013, the Maine legislature voted to significantly restrict the board's authority to release confidential and patient identifying data. Originally, the board has the authority to release Level III data containing identifiable patient information to the Department of Health and Human Services and "other researchers," for research purposes as long as the proposed use and storage appropriately safeguarded confidential or privileged information.[106] Under the new provisions, effective in July 2016, MHDO can only release Level III data to public health authorities, not other researchers, and only for purposes "mandated by state or federal law," greatly reducing the scope of analysis possible using MHDO data. The Maine legislature also repealed provisions granting the board significant power to act in the public's interest to both release and protect information contained in the MHDO. The legislature previously specified that the board may not approve any release of information that would violate any state or federal law or diminish the confidentiality of health care information or the public's confidence in the protection of that information in a manner that "outweighs the expected benefit to the public of the proposed investigation."[107] This provision granted the board leeway to both

---

[103] 90-590-120 ME. CODE R. § 3(1)(E)(2017).

[104] 90-590-120 ME. CODE R. § 3(1)(F-H)(2017).

[105] 90-590-120 ME. CODE R. § 3(1)(D)(2017).

[106] The legislature required that MHDO ensure that: 1) identifying information is only used to gain access to medical information pertaining to public health; 2) patients provide consent, unless the information sought is only for verification or comparison of health data, and the board finds that confidentiality can be adequately protected without patient consent; 3)researchers do not further disclose identifiable information without the patient's consent; 4) identifiable information is used to the minimum extent necessary to achieve the goals of the approved research; and 5) research protocols are designed to preserve confidentiality of all identifiable health care information and maintain public confidence. 22 Me. Rev. Stat. § 8707(3)(B)(2017).

[107] 22 Me. Rev. Stat. § 8707(3)(C)(2017).

protect the data, as well as release it when doing so would be in the public interest. Finally, with respect to financial information, the legislature repealed the board's discretion to determine whether financial data submitted under §8709 constituted confidential information, in instances where public disclosure of the data will result in the provider being competitively disadvantaged.[108] This provision did not require the Board to deem any competitively disadvantaging information confidential, it merely give the Board the option of doing so. Its repeal, however, grants health care provider organizations and payers great ability to keep negotiated payments and charges concealed in ways that may hinder the effectiveness of health care cost control efforts. It will be interesting to see how these changes impact the use and analysis of data collected by the MHDO.

Massachusetts

The Massachusetts APCD legislation establishes strict constraints on the release of personal health information.[109] The legislation permits providers, provider organizations, public and private payers, government agencies and authorities, as well as researchers access to de-identified data.[110] Similar to Maine, the Massachusetts legislation limits the usage of APCD data for specific purposes. Massachusetts permits access to de-identified data only when the purpose of the data request is for lowering medical expenses, coordinating care, benchmarking, quality analysis, and "other researcher, administrative or planning purposes." Identifiable data, according to the legislative language, can only be released when necessary for a government agency or authority to achieve its public purpose or to providers and payers for the purposes of treatment and coordinating care. As such, the Massachusetts legislation appears to establish a broad restriction on researchers' ability to access data for analysis. However, unlike other states, Massachusetts has the Health Policy Commission with a staff of health economists and health services researchers who perform much of the research needed for state health policy. Further, despite the seeming restrictiveness of the Massachusetts legislation regarding the release of identifiable data, the regulations governing the Massachusetts APCD establishes processes and procedures that appear to allow researchers to obtain identifiable data and providers and payers to obtain identifiable data for purposes other than treatment and care coordination.[111]

Prior to any final decision on the release of data to non-governmental applicants, the Data Privacy Committee (DPC) and the Data Release Committee (DRC) must review the applications. Both the DRC and DPC are established by regulation and are charged with reviewing applications to ensure that

---

[108] 22 Me. Rev. Stat. § 8707(4) (2017).

[109] Mass. Gen. Laws. c. 12 § 12(2017).

[110] Mass. Gen. Laws. c. 12 § 12(b)(2017).

[111] The authors have also spoken with representatives of CHIA, who have confirmed that under certain conditions, researcher may obtain identifiable data. In addition, the CHIA website makes available pending applications for data, which appear to show the presence of applications from researchers for identifiable data.

the proposed use of the requested data is in the public interest and that applicants have met the regulatory burden for data disclosure.[112] Members of the DRC are to be non-CHIA personnel, including payers, providers, consumers, researchers, and advocacy groups.[113] The DPC members must be CHIA personnel or contractors with experience in data privacy, data security, information technology and research.[114] After reviewing the applications, both committees then make non-binding recommendations to the Executive Director.

Colorado

In specifying data release restrictions and procedures, the Colorado legislation does not directly refer to de-identified or identifiable data.[115] Even in the absence of such terminology, the Colorado legislation, by subjecting the release of APCD to the requirements of HIPAA, places robust restrictions on the release of such data. HIPAA places broad restrictions on the unauthorized release of PHI. HIPAA also, however, establishes certain exceptions that permit the release of identifiable data in the absence of a written patient authorization. The relevant exceptions permit disclosures required by law, for the health oversight purposes, and for research purposes. The enactment of APCD legislation requiring release under certain circumstances would presumably allow for the disclosure of data under the "required by law" exception. The HIPAA exception for the disclosure of PHI for research purposes further elaborates a set of protocols and procedures that researchers must satisfy prior to the disclosure. HIPAA also requires data recipients to provide assurances, including that they will not reuse or disclose except under certain circumstances, they have or will obtain approval from an IRB or privacy board, the research requires the requested disclosure, they have a plan to protect against improper use or disclosure, and they have plan for the destruction of data at the termination of the proposed research.[116]

In Colorado, HIPAA only establishes the minimum level requirements for the release of data. The Colorado legislation empowers the executive director, with the input of the advisory committee, to establish additional procedures and requirements for the release of APCD data.[117] Subsequent sections of the Colorado legislation create additional requirements and restrictions. Section seven specifies that that the APCD database shall be available to insurers, consumers, employers, providers, purchasers of health care, and state agencies when released in a "form and manner" that protects the privacy and security of personal health information. While the legislation did not use the terminology "de-

---

[112] 957 CODE MASS. REG. 5.07 (2017); 957 CMR 5.06(8)(2017).

[113] 957 CODE MASS. REG. 5.07(2) (2017).

[114] 957 CODE MASS. REG. 5.06(8) (2017).

[115] COLO. REV. STAT § 25.5-1-204(2017).

[116] 45 C.F.R. 164.502(i)(2017).

[117] COLO. REV. STAT § 25.5-1-204 (2)(b)(I); (5)(e) (2017).

identified" data, this section appears to create restrictions and procedures for the release of de-identified data. The Colorado legislation, like that in Massachusetts, specifies that the purposes for which such de-identified data shall be released will include the review of health care utilization, expenditure, and quality and safety performance in Colorado.

A subsequent clause of section seven also includes language making APCD data available to state agencies and private entities in Colorado engaged in efforts to improve health care. The absence of language specifying that data released under this provision be in a "form or manner" that protects privacy and security implies that such data released to state agencies and private entities in Colorado may be identifiable. The language is, however, vague in regards to identifiable data and restricts the release of data under this provision to only state agencies and private entities in Colorado.[118] This language not only restricts the release of identifiable data to entities based in Colorado, but would also seemingly exclude researchers at public universities in Colorado if public universities are not classified as state agencies or private entities.[119] The legislature created further uncertainty regarding researchers and their access to APCD data by omitting any mention of "researchers" as a category of data recipients within the legislation. Ambiguity in the statute results in a great deal of uncertainty regarding who may access APCD data and for which purposes within Colorado. While regulations and APCD policies and procedures may serve to ameliorate some of this uncertainty, clarity and specificity in statute language will better preserve the legislature's intent over time.

New York

The New York APD legislation establishes the broadest framework governing the release of APD data. One of the initial responsibilities given to the commissioner in the New York legislation is the responsibility of protecting the confidentiality of patient-identifiable data.[120] A later provision specifies that the commissioner establish regulations to ensure the protection of patient privacy in the collection, publishing, release, use, and access to APD data.[121] Unlike Maine, Massachusetts, and Colorado, the New York legislation provides no specificity regarding different access procedures and requirements for identifiable or de-identified data or for different categories of requestors. In Colorado, only government agencies and private entities in Colorado can request identifiable data. In Maine, providers, payers, and

---

[118] COLO. REV. STAT § 25.5-1-204 (7)(b) (2017).

[119] The Colorado regulations, however, offer a slight variation on these legislatively defined restrictions. The regulations, for example, specify that state agencies and private entities may request a "specialized report" if the state agency or private entity is engaged in efforts to improve health care or public health outcomes in Colorado. The regulations replace the requirement that the entity be based in Colorado with the requirement that the entity be engaged in research aimed at improving health in Colorado. Colo. Code Regs. §1.200.5.A.(2017).

[120] N.Y. Public Health Law § 2816(1)(a)(2017).

[121] N.Y. Public Health Law § 2816(2)(b)(2017).

their business associates (as defined in HIPAA) may request identifiable data for treatment, payment or health plan operations. In Massachusetts, the legislation treats providers, payers, researchers, and government entities differently when granting access to identifiable data. The Massachusetts legislation also restricts the purpose for which data can be requested. Other than a provision that specifically allows access to a provider for the purposes of treating a patient, the New York legislation does not include any similar restrictions or specific procedures to that seen in Maine, Massachusetts and Colorado.[122] The relatively minimal clarity and specificity regarding data release in the New York legislation gives considerable authority and discretion to the commissioner and the advisory council to establish privacy and security protections in the release of data. The broad level of discretion granted to the commissioner provides flexibility, speed of action, and expertise in drafting data release regulations, but it also leaves patient privacy in greater limbo as no legislative floor of protection exists.

Recommendations

We recommend that the California legislation make the release of APCD data subject to HIPAA and CMIA. As was true for security and privacy procedures, HIPAA and CMIA would set only the minimum restrictions and requirements for the release of APCD data. The California legislature or the Secretary, acting with input from the advisory committee, could then enact or issue additional APCD-specific data release provisions that would establish stronger protections and more rigorous procedures for the release of data.

Both HIPAA and CMIA establish broad constraints on the disclosure or release of personal medical information without the authorization of the patient in question. HIPAA and CMIA, however, also establish exceptions that allow for the disclosure of PHI in the absence of authorization from the affected patient. The exceptions, as stated above, include disclosures required by law and for certain research purposes, with the latter subject to additional constraints and data safety requirements.

CMIA also places a particularly strong constraint on the re-disclosure of personal health information.[123] The restrictions on the re-disclosure of medical information apply to any person or entity that receives medical information under a CMIA authorization. If an ACPD was subjected to CMIA, the provisions restricting the re-disclosure of medical information would apply to any entity or person that receives data from the APCD. Researchers, for example, would face tight restrictions on any subsequent use or disclosure of data. The restrictions placed on the re-disclosure of medical information, therefore, apply beyond the providers, employers, and third-party administrators that CMIA initially targets. For any re-disclosure of medical information, CMIA requires prior authorization from the patient or the patient's representatives.[124] The procedures and requirements for obtaining

---

[122] N.Y. Public Health Law §2816(4)(2017).

[123] Cal. Civil Code § 56.13 (2017).

[124] The authorization must be obtained pursuant to section 56.11, which requires any re-disclosure follow the procedures set forth by section 56.13. Cal. Civil Code § 56.11-13 (2017).

authorizations for re-disclosures, therefore creates tighter constraints on the release of medical information than that established for the initial disclosure of medical information.

We also recommend that legislation include a direct and explicit discussion of de-identified and identifiable data. Among the states reviewed here, legislation often created unnecessary confusion as a result of legislative language that did not clearly establish an explicit demarcation between the different approaches to identifiable and de-identified data. We further recommend that the legislation specifically outline the categories of actors that may request identifiable and de-identified APCD data, as well as specify the purposes for which data may be requested. The legislation should also provide individuals the opportunity to opt out of having their identifiable data released for research without their consent. To add additional oversight and protections for the release of identifiable data, we recommend establishing a committee to oversee and review requests for identifiable data. A similar data review committee was established through the regulatory process in Massachusetts, but by establishing such a committee through legislation, California would provide explicit assurances that the release of any identifiable data would undergo a rigorous review by a panel comprised of internal and external experts.

Conclusion

Overall, we recommend that California establish an All Payer Claims Database designed to collect all health care claims data within the state to promote transparency, informed decision making, and improve health and healthcare for all Californians. We recommend that the legislature do so in a manner that provides robust protection for personal health information while enabling policymakers, researchers, and public health authorities reasonable access to the data collected by the APCD to promote improvements in health and health care throughout the state. We recommend the creation of an independent oversight body with a broad membership appointed by a range of individuals and organizations to ensure diversity and expertise within its membership. At a minimum, the legislature should subject the APCD to the requirements of HIPAA and CMIA, as though it were a covered entity. These requirements provide a solid baseline for privacy protections, while granting the oversight body or the Department of Health and Human Services the option to increase the stringency of the requirements as needed.