Financialization through Health IT, Part II: From Electronic Health Systems to AI

Rosemary Batt
Alice H. Cook Professor of Women and Work
Global Labor and Work and HR Studies
ILR School, Cornell University, Ithaca, NY 14853
rb41@cornell.edu

Eileen Appelbaum, Co-Director
Center for Economic and Policy Research
1611 Connecticut Ave. NW Suite 400
Washington, DC 20009
appelbaum@cepr.net

February 11, 2025

We are grateful to Arnold Ventures for financial support, and especially Hunter Kellett and Alexandra Spratt for their ongoing intellectual interest and project guidance. The report benefited from the able research of Emma Braff, Kristie Chu, Hyeon Joo Lim, Adam George Rose, Anmol Sethi, Daniel Smith, and Francia Togba. We also thank Diane Bailey, Dean Baker, and Adam Seth Litwin for their comments.

Executive Summary
Financialization through Health IT, Part II: From Electronic Health Systems to AI

Rosemary Batt and Eileen Appelbaum

The heightened role of private equity in extracting wealth from healthcare services has captured national attention in the media and academic research – with the massive bankruptcy of the Steward Healthcare System the poster child for 2024. Private equity firm Cerberus bought out Steward in 2011, sold off its property, cut staffing and supplies, extracted over $1 billion, and ran it into bankruptcy by 2024.

Much less sensational and hidden from view are many other financial actors who own and operate other parts of the healthcare sector.

In this two-part report, we examine the federal laws governing health IT and the cluster of firms that create, own, and operate the information infrastructure that healthcare providers depend on. These include venture capitalists, health IT vendors, and 'Big Tech' firms from Silicon Valley as well as private equity firms and other Wall Street actors. While health IT systems have become embedded in provider organizations as essential to decision-making processes, little attention has been paid to whether or how this change has increased healthcare financialization. By financialization we mean the extent to which actors with primarily financial interests penetrate the industry and shift the logic of decision-making and its outcomes away from its healthcare mission and towards financial goals. The answers to these questions are important for the current debates over what standards and guardrails should be adopted for AI and machine learning in healthcare.

The empirical question is whether these financial actors are *creating value* for healthcare more than they are *extracting value* from it. We begin with the observation that health IT may create value for clinicians and patients and enrich the firms best situated to profit from the technology. Whether this financial relationship enhances or limits the technology's potential to improve healthcare delivery systems depends on the laws and regulations put in place to set standards and enforce them, the conditions under which it is implemented, and who has the relative power to set prices and quality. We are interested in the extent to which health IT has improved healthcare relative to its potential, how much external financial actors have extracted wealth from it, and whether this has come at the expense of healthcare organizations, employees, patients, and taxpayers.

This question is particularly salient now as the issue of artificial intelligence (AI) and machine learning (ML) in healthcare has come center stage and policymakers are debating how to regulate them. There is great enthusiasm that these technologies will cut costs and improve health care quality, while there also is great concern about accountability and the ability to

regulate their use. The current public debate echoes that of thirty years ago over whether electronic health records (EHR) would achieve cost and quality improvements.

In Part I, we examine the evolution of electronic health record systems, and their adoption based on an analysis of the laws, regulations, and empirical evidence on their use and outcomes over several decades. We reconsider the widespread assumption that health IT has reduced healthcare costs and improved efficiencies. Who are the leading actors in this domain? What are the relationships between health IT financiers, vendors, and healthcare provider organizations? Who has benefited, and who has borne the risks and costs of EHR implementation? To what extent have regulatory guardrails succeeded in providing transparency, accountability, and protections against EHR system failures or deficiencies?

Part II of the report considers a broader set of developments in health IT, including the role of venture capital, private equity, IT vendors, and Big Tech companies in the development of integrated health IT systems that healthcare organizations increasingly depend on. EHR platforms became the foundation for layering on software systems for claims and revenue cycle management (RCM), data analytics, algorithmic decision-making, and AI and machine learning applications. The rapid development of these 'end-to-end' management systems that integrate patient data into financial accounting systems has positioned them to serve as the infrastructure for embedding AI and machine learning tools into healthcare decision processes – without prior safeguards or input from patients and healthcare workers and without regulatory standards, transparency, or safeguards. The federal government's late-stage efforts to weigh in on AI applications in healthcare face a powerful set of financial players with deep stakes already planted in healthcare. Again, the empirical question is who benefits and who absorbs the risks and pays the costs? Our analysis of the evolution and unintended consequences of health IT informs the current debates over regulating these recent developments in health IT.

In Part I, the findings from this research point to the important role that the federal government has played in mandating and subsidizing the adoption of health IT systems – but without providing sufficient guardrails or oversight to ensure that taxpayer dollars have been used to benefit clinicians, patients, payers, or the Medicare Trust fund. As a result, the evidence suggests that health IT financiers and vendors often have benefited at the expense of other stakeholders.

The evidence suggests that these outcomes are the result of an underlying faith that information technology, now including AI, is the key to reducing costs and streamlining the delivery of healthcare services. This belief took off as the digital revolution emerged in the 1980s and 1990s. The Clinton administration pushed through the 1996 HIPAA legislation in order to protect patient data privacy and support healthcare portability, which set the stage for standardized electronic patient records as well as billing systems. George W. Bush institutionalized federal support for health IT by establishing the Office of the National Coordinator for Health Information Technology (ONC), and in 2009 the Obama Administration mandated that

healthcare organizations adopt EHR systems, providing billions of dollars of subsidies to do so under the HITECH Act. Features of the Affordable Care Act (ACA), as well as the federal push to adopt value-based care (VBC), have added incentives for the adoption of EHR systems.

But none of these laws and regulations provided guidelines for testing, monitoring, or regulating the use of IT in healthcare, nor did they offer protections for workers' rights or funding to train employees in the use of health IT. Taxpayer dollars that subsidize the adoption and upgrading of health IT flow like water through healthcare organizations to a host of tech vendors, private equity firms, data mining and marketing companies, revenue cycle management firms, data analytics firms, and others.

The strengths and limitations in the HIPAA privacy rules, as amended under the HITECH Act, produced intended and unintended consequences. The HIPAA privacy regime offered major protections for patient electronic data privacy, limiting access to healthcare providers and payers. But it also allowed access to patient data by 'business associates' that provided services to providers and payers. As the health IT 'ecosystem' grew, hundreds of enterprises gained access to private patient health information, without patients' full knowledge and often without any strong justification for their 'need to know.'

The assumed cost effectiveness of health IT that fueled passage of the HITECH Act did not receive sufficient empirical scrutiny before federal adoption mandates were in place and billions of taxpayer dollars had been spent. While the mandates successfully ushered in rapid adoption of EHR systems, the systems were flawed, user-unfriendly, and lacked interoperability (the ability of EHR systems to share information), which was one of the central requirements of the HITECH law. As a result, healthcare organizations became laboratory sites for experimentation in which providers and patients often bore the costs of health IT glitches, inaccuracy, and lack of interoperability. Health IT lacks public oversight and guardrails, allowing venture capitalists and IT vendors to make billions on the adoption of unproven technologies by health provider organizations.

The HITECH adoption mandates led to 'a rush to adopt' EHRs, which also privileged the legacy IT vendors – allowing them to acquire asymmetric market power (and in some market subsegments, monopoly power), which has allowed them to charge high prices. Federal subsidies to support innovative startups, by contrast, did not emerge. The market leaders often maintained their dominance through anti-competitive strategies such as information blocking, through which they undercut federal guidelines for interoperability or charged high fees to physicians, clinics, or other users to link to their systems. It wasn't until 2016 that Congress passed the 21st Century Cures Act, which mandated standards for interoperability for health IT developers and put in motion a national framework for health data exchange under the Trusted Exchange Framework and Common Agreement (TEFCA). Final regulations of the Cures Act were posted in May 2020,

while those for TEFCA took until 2024. Fifteen years after the HITECH Act, 30 years after HIPAA, and 60 years after EHR innovations emerged, interoperability is viewed as 'promising.'

Empirical evidence shows that EHRs have led to better billing processes and internal communications in provider organizations, but not necessarily cost savings. That is because few studies calculate total economic costs that include the hidden costs of installing, maintaining, and upgrading systems – as well as hiring, training, and retraining the entire healthcare workforce to be proficient in data management as these systems continually change. Large healthcare systems spend billions of dollars on EHRs while smaller hospitals are pressed for resources to install or maintain them.

A primary expectation among medical practitioners and EHR advocates was that EHRs would substantially reduce or eliminate medical errors due to human data input and updating, but hundreds of empirical studies from the 1990s to the present have found that inaccurate or outdated information is often embedded in patients' EHRs. While both manual and electronic systems are subject to human errors of data entry, EHR systems encourage widespread use of cut-and-paste features, which may lead to the persistence of outdated information in patient records, information overload for physicians, delays in care, or more serious threats to patients' lives.

The unanticipated negative outcomes of EHRs for physicians, nurses, and frontline workers are also well documented since the 1990s. As EHR systems became more complex, the data entry requirements for physicians and healthcare workers also increased, leading to excessive time spent by physicians on computers rather than direct patient care – with additional hours at home finishing up documentation. Physicians and nurses continue to report that systems are onerous, usability is low, much information is irrelevant or redundant, and the inefficient use of their time for clerical work has grown immensely – leading to high and growing quit rates. Information overload leads to cognitive overload, at times undermining patient care or safety. None of these costs are well understood or integrated into cost-benefit analyses of the value of health IT.

The findings in Part II of this report identify the process through which EHR systems became the platforms for integrating claims and financial management systems, or end-to-end revenue cycle management. While the legacy IT vendors Epic and Oracle Cerner diversified their revenue streams into claims and financial management systems, private equity firms bought out independent RCM companies, accelerating their acquisitions in the 2020s as the potential to further automate systems via AI and machine learning took shape. In addition to collecting medical debt via revenue cycle management companies, private equity firms have also bought up medical loan and credit card companies that often result in low-income patients paying more than they otherwise would have. The unanticipated developments in health IT over three decades have had – and continue to have – consequential outcomes for patients, clinicians, healthcare provider organizations, and the costs and quality of care.

Thus, a direct line of sight exists between the creation of EHR systems in the 1990s, their mandated use in 2008, their linkage to financial management systems in the 2010s, and their position today as laboratories for testing data-driven decision-making. Venture capital, private equity, and Big Tech have financed a range of firms using data analytics to experiment with cost management, risk management, algorithmic decision-making, 'value-based care enablement', and more recently AI and machine learning.

The platforms are virtually unregulated, with no independent process to scrutinize them before they are used in healthcare systems and no guardrails against potential downside risks for patients. They are non-transparent, making it extremely difficult to assess whether AI is being used for cost saving or cost-shifting from insurers or healthcare systems to employees and patients. Early research has identified several major concerns over algorithmic and AI-driven decision-making systems. These include the inaccuracy and biases of data that AI uses, leading to improper diagnoses or care recommendations; racial and economic bias embedded in AI systems; the use of AI 'recommendations' as strict rules to be implemented; the hidden ways that data analytics may be used to shift costs from hospitals and insurance companies to healthcare providers and patients. In the meantime, Wall Street, Silicon Valley, and Big Tech actors are making billions selling data and AI systems that lack sufficient testing, transparency, or regulation.

The proprietary ownership of massive databases of patient health data has also raised major concern over its use for marketing purposes and private gain. While HIPAA privacy rules were designed to protect individual patient data, they also allowed 'de-identified' data (stripped of personal identifiers) to be used for secondary purposes, such as medical research or population health management. Following passage of HIPAA, however, large ad agencies and data mining companies that pre-dated HIPAA were well-positioned to take advantage of de-identified data to monetize it for marketing and private research. The unintended consequence is the growth of an unregulated multibillion-dollar industry in monetizing patient data for private gain without patients or healthcare providers' knowledge.

Because de-identified data is costly and held by large EHR vendors and insurance corporations, academic medical researchers often do not have access to it. Instead, it is often sold to large data analytics and private research or pharmaceutical companies that do not have to follow traditional medical ethics standards and clinical research protocols. Given the proprietary nature of the data, studies cannot be replicated — and it is unclear whether this research meets scientific standards or not. The complete lack of transparency means that the public cannot assess the extent to which patient data is being used for private gain versus the public good.

A related and ongoing concern is patients' privacy rights. As EHR has become the basis for integrating end-to-end revenue cycle management, hundreds or thousands of entities now have access to a patient's personal health information: The ecosystem of healthcare organizations,

providers, insurers, tech vendors, and related businesses with access to personally identifiable information has grown substantially over time. These actors can sidestep the protections in the well-intentioned but flawed HIPAA and HITECH Acts. Patients' rights advocates are particularly concerned about the extent to which sensitive mental health and other personal information can be accessed by entities without a clear 'need to know.' A related concern is that de-identified information may be re-identified, as shown in a growing number of empirical studies using advanced data analytic techniques.

Moreover, the linkage of medical and financial records in end-to-end systems has made healthcare by far the most vulnerable industry to cyberattacks due to the high value of this sensitive information on the black market. Between 2009 and December 2024, data breaches affected some 748.5 million individual healthcare records. The number of data breaches of 500+ health records in provider organizations more than doubled between 2018 and 2023, and the 2024 Change Healthcare breach alone affected over 100 million individuals. Since 2020 the costs of healthcare data breaches have increased by 53.3 percent. In sum, the unregulated expansion of health IT infrastructure by financial actors has launched unparalleled demand for cybersecurity systems. Healthcare organizations must now invest billions more in cybersecurity systems, which are owned and operated by venture capital, private equity, and Big Tech firms.

Part II Table of Contents

Financialization in Integrated Health IT Systems

The integrated health IT systems of today build on decades of experimentation with electronic health records systems in healthcare organizations, fostered and subsidized by the federal government. As described in Part I of this report, the growth of EHR systems in the 1990s under the HIPAA Act and their mandated use under the HITECH Act of 2008 was fraught with ongoing problems. Venture capitalists, IT vendors, and Big Tech Silicon Valley firms made billions by installing often unproven IT systems in healthcare organizations with little federal oversight or technical or financial transparency. Provider organizations, physicians, nurses, and workers more often than not absorbed the risks and costs of system glitches, time-consuming data entry, and workarounds – at times undermining patient care. EHR system failures have been a major source of burnout and high quit rates for healthcare workers, long before the COVID-19 pandemic. Federal lawmakers provided no consultative or technology rights for workers, nor funds for training and skills upgrading.

The costs of system installation and maintenance have been unexpectedly high, due in part to the concentrated market power of select health IT vendors and the high costs of switching systems if one vendor fails to deliver. Moreover, the total hidden costs of their implementation – including ongoing training and retraining of employees to handle system upgrades or time away from patients – have not been calculated.

In Part II of this report, we review the developments of federal laws and regulations governing health IT since passage of the HITECH and Affordable Care Acts. We assess the extent to which this regulatory framework shaped the activity of financial actors in health IT, including venture capital, private equity, IT vendors, and Big Tech. How have federal laws shaped the application of revenue cycle management, data analytics, algorithmic decision-making, and artificial intelligence in healthcare? What are the implications for provider organizations, healthcare professionals and workers, and patients? Here, we focus on the privacy and security of patients' health data in the context of the lightly regulated health IT industry. Two arenas are particularly problematic: The explosive growth of the patient data mining and marketing industry, and the ongoing threats of data breaches and cybersecurity threats in healthcare – the most vulnerable of any industry.

Revenue Cycle Management Systems

Revenue cycle management (RCM) systems have contributed to healthcare financialization, as the growing dependence of healthcare organizations on these systems has attracted venture capital, private equity, IT vendors, and Big Tech to this market niche. Of the largest RCM

vendors in 2024, the top three are Epic, Oracle Cerner, and Meditech – legacy IT vendors which used their EHR platforms to integrate RCM services, retain their current client base, and further expand their market share. Five of the other largest or fastest growing RCM vendors are private equity-owned or formerly PE-owned.

RCM systems are now the glue that links the standardized coding in patent health records to billing, financial accounting systems, claims management, and bill collecting. Because financial actors have built these systems into massive, centralized health IT data hubs, they have made them the most valuable and vulnerable for hacking and cyberattacks of any industry's data systems, including financial services, which we discuss in the last section of this report.

RCM companies began as simple billing and accounting software programs that turned paper records into electronic ones. They developed in separate but parallel tracks with electronic health records (EHR) during the 1990s and 2000s, when they rebranded themselves as revenue cycle management in the 2000s. As documented in Part I of this report, a key advantage of EHRs was their improved billing accuracy, facilitated by standardized codes and clinical documentation. By the mid-2000s, RCM companies began capitalizing on the advances in billing and coding found in electronic health records, while hospital demand for outsourced RCM systems grew due to the rise of uncompensated care costs and the Great Recession.

The passage of the HITECH and Affordable Care Acts stimulated demand to link EHR systems to RCMs in 'full cycle' or 'end-to-end' revenue cycle management. In the 2010s, RCM systems started diversifying their services, integrating a wide range of functionalities into their platforms – from initial patient contact to the completion of claims and payments (Hansei 2024). Currently, the most advanced companies include services for registering patients and collecting their full personal, financial, and health information; scheduling visits and verifying insurance; coding and documenting diagnoses (using the International Classification of Diseases, or ICD) as well as medical procedures (using the Current Procedural Terminology, CPT); processing payments, tracking claims, and evaluating claims denials; and billing and collecting payments from patients. A further extension involves monitoring performance metrics, such as claim processing, revenue generation, and reimbursement rates (Kieffer 2023).

The heightened demand for outsourced RCM systems after 2010 attracted more venture capital and private equity firms to the market, which accelerated in the second half of the decade. In the 2020s, exuberance over the potential for AI and machine learning to streamline information processing and reduce administrative burden has led to a flood of new financial actors in the RCM niche market (LaPointe 2023).

Federal Laws Spur RCM Market Growth

The passage of the HITECH Act and the Affordable Care Act spurred market demand for RCMs. Once EHRs standardized coding systems were in place, integrating RCM systems became more

valuable and potentially cost-effective. The ACA helped to expand demand for integrated EHR-RCM systems as hospitals began treating millions of additional people who gained health insurance through local health exchanges markets. These plans featured high deductibles, and employers also began switching to higher deductible plans. Patients are responsible for initial bill payments under these plans, which made hospital bill collecting more uncertain and time-consuming. The Obama administration also reduced the growth rate of Medicare reimbursements, squeezing hospital margins. Pent up demand from lack of insurance and income loss following the Great Recession led to large increases in the volume of patients that hospitals treated. With many families living paycheck to paycheck, they fell behind on medical bills, and RCM bill collectors pursued them.

In addition, the ACA and subsequent CMS regulations have pushed the adoption of capitated or value-based payment (VBC) models, which also spurred demand for integrated EHR-RCM systems. VBC models reimburse hospitals at a prescribed level of payment for a given procedure – allowing hospitals to keep the profit if their costs come in below that (upside gains) or lose it if there are cost-overruns (downside risks). CMS has also extended these models to all types of provider organizations. EHR-RCM platforms are more valuable under VBC payment systems because their complexity requires healthcare organizations to document a broader array of cost and care quality metrics, which is very difficult without the use of RCM systems.

Moreover, the 21st Century Cures Act, which pushed IT vendors to comply with interoperability standards, provided legacy vendors like Epic and Cerner to expand their platforms to include RCM systems in order to raise revenues and retain already captured clients. The hospital price transparency rule, which went into effect in January 2021, requires hospitals to post machine-readable files with data on prices they negotiated with payers, including gross charges and discounted cash prices for 300 shoppable services (CMS 2024). This new requirement adds another incentive for hospitals to adopt integrated RCM systems. While compliance in the first year stood at roughly 25 percent of all hospitals, that figure climbed to about 75 percent in 2024 due to heightened penalties for non-compliance (from a maximum yearly fine of $110,000 up to the current fine of more than $2 million for larger hospitals that do not comply). As of spring 2024, 14 hospitals had received fines, while 1,000 had received warning notices. Fines have ranged from $57,000 to $979,000, but some hospitals have opted to pay a fine rather than report prices (Kacik 2024).

The heightened demand for full cycle RCM systems has, in turn, fueled exuberance over potential cost savings and experiments with AI integration into RCM systems. Industry insiders are vigorously promoting AI via commissioned surveys and reports. A 2020 study sponsored by Change Healthcare – whose 2024 cyber security breach exposed one-in-three American's records – surveyed 200 'leading experts' in IT, RCM, and healthcare finance. It reported that two-thirds of hospital and healthcare systems were currently using AI in RCM, and that by 2023, 98 percent of healthcare leaders anticipated using AI in RCM in some form (Businesswire 2021).

A 2021 survey by industry consulting firm AKASA reported that 78 percent of health systems were currently using, or were in the process of implementing, automation in their RCM operations – a 12 percent increase over the prior year (Hagland 2021).

While it is far too early to know whether or to what extent AI and machine learning will produce labor-saving efficiencies, venture capital, private equity, IT vendors, and Big Tech are pouring into AI in health IT in expectation of extracting billions. Investment bank analysts report that health systems spent on average 14.1 percent of their health IT budgets on RCM systems, and they expect that percentage to increase (Delancey Street Partners, LLC 2022). In 2023, the size of the US RCM market was estimated at $155.6 billion, and projected to grow at a compounded annual rate of 10.2 percent between 2024-2030 (Grand View Research 2023).

Private Equity in the RCM Market

The financial activity of private equity and venture capital owners was undeveloped in the 2000s but grew steadily in the 2010s (Appelbaum and Batt 2020).[1] It surged in the 2020-2025 period, due to the pandemic and exuberance over potential big profits through AI and machine learning. In the 2000s, two investor-owned hospital systems were early leaders: Parallon, a subsidiary at Hospital Corporation of America when it was private equity-owned, and Conifer Health Solutions at Tenet Healthcare. Both developed in-house administrative services and then expanded profits by offering outsourced systems to other investor-owned, as well as nonprofit, hospital systems. Both Parallon and Conifer continue to be leading players in the RCM segment – using their early expertise to diversify beyond RCM platforms and offer consulting and business office services, financial risk management, population health management, and other administrative functions for external clients (PitchBook Conifer 2025; PitchBook Parallon 2025).

Private equity firms were attracted to the RCM market in the 2010s because it was fragmented, with hospitals typically using different contractors for different parts of the financial management cycle. Some PE firms already owned IT companies that could serve as platforms (Loyale Healthcare 2019). Hospital demand for integrated RCM systems grew substantially – by 86 percent between 2015 and 2018, according to one industry survey. It reported that the number of hospitals implementing full RCM outsourced projects grew from 11 to 18 percent in that period (LaPointe 2018).

Private equity and venture capital backing of RCM vendors grew at a rate of about 10 percent per year in the 2010s, according to PitchBook data. Private equity backed about 50 percent of first financing deals, and venture capital about one-third. Almost 80 percent of the PE deals were leveraged buyouts. Large buyout firms such as Blackstone, Thomas Lee Partners, Vista Equity, Thoma Bravo, The Gores Group, and Waud Capital Partners entered the market. However, annual RCM deal activity more than doubled between 2020 and 2024, as the RCM market was

one of the most stable in healthcare during the pandemic and exuberance over AI applications surged. As of July 2024, 199 RCM companies were PE- or VC-owned or formerly owned, including 104 current PE-backed companies (78 percent via LBOs) and 61 current VC-backed companies (PitchBook data, authors' calculations).

While the legacy IT vendors (Epic, Oracle Cerner, and Meditech) were well positioned to quickly dominate the end-to-end RCM market, private equity has acquired among the largest and fastest growing RCM companies in the US – including Athenahealth, FinThrive, NextGen, AGS Health, R1 RCM. Each company has gone through a series of leveraged buyouts from one PE firm or consortium to another, according to PitchBook data. For example, Athenahealth was acquired in a $17 billion leveraged buyout in 2022 by a PE consortium led by Helman & Friedman and Bain Capital. They bought it from PE firms Veritas Capital, Elliott Investment Management, and Ares Capital (which continued as an owner), who had acquired it in a 2019 LBO for $5.9 billion. Prior to that, it grew through over a dozen acquisitions backed by private equity and a dozen startups with VC financing. Private equity firm Pamplona Capital built FinThrive through a series of LBO add-ons before selling it to a consortium of PE firms in a 2021 leveraged buyout. PE firm Thoma Bravo took over NextGen in a 2023 LBO for $1.8 billion. It had grown through over 20 M&As that added on a range of diversified health IT services. AGS Health was acquired by PE firm BPEA EQT in 2019 from another PE consortium, which acquired the company in 2017.

The formerly PE-owned RCM companies are Parallon (the HCA subsidiary) and Change Healthcare (currently owned by UHG and previously owned by PE firms Blackstone and Hellman & Friedman). R1 RCM was taken private in 2024 in a $8.9 billion leveraged buyout by the private equity arm of Ascension Health System (the country's largest Catholic hospital system), TowerBrook Capital Partners, and Clayton, Dubilier & Rice. TowerBrook and Ascension already owned 36 percent of the company, and Ascension is R1's largest customer, accounting for 40 percent of the company's revenues (Herman 2024). The current state of private equity in RCM is well documented in a 2024 investigative report that details a series of case studies of PE leveraged buyouts and aggressive M&A activity in the 2020s (Fenne 2024).

Provider Experiences with Outsourced RCM Companies

RCM companies promote outsourced solutions as a pathway for healthcare organizations to reduce attention and resources for financial management and dedicate more to patient care. They claim that patient satisfaction increases when RCM is outsourced because the RCM company is better able to accommodate what patients want, such as 24/7 customer service and other consumer-focused operations (Schmidt 2016).

The empirical evidence that outsourced RCM systems have delivered on their promises is thin, with industry consultants regularly pointing to "healthcare providers' ongoing struggles with … RCM inefficiencies" (Ak and Verma 2024). Industry surveys show provider organizations have had substantial dissatisfaction with outsourced RCM vendors, as in KLAS's Outsourced Revenue Cycle Services 2019 market report. It found that one-third of the 140 healthcare organizations surveyed would not purchase their vendor's RCM services again. That finding was substantially higher – 70 percent – for Cerner, the worst performer. Many of the top outsourced RCM companies, including those owned by private equity, experienced double-digit declines in satisfaction rates between 2017-2019. Clients cited companies that 'nickel-and-dimed' them, 'oversold services offered,' used 'cookie-cutter' approaches, were 'slow to work,' and provided insufficient staffing and few consequences if they underperformed (Zeitner 2019). A 2024 survey of 115 healthcare system executives by a different independent research firm found that only 36 percent said their outsourced RCM vendor was at least 'somewhat effective,' while 3 percent said it was 'extremely effective.' In comparing the three largest EHR vendors that also offer RCM services, only 29% of survey respondents said Epic met their RCM needs "very well" or "extremely well," versus 19% for Meditech, and 9% for Cerner (Sage HarrisWilliams 2024).

Another industry benchmarking study compared in-house to outsourced RCM systems and found few benefits to outsourcing. In-house systems had slightly lower rates of patient payments at point-of-service (16.5 percent compared to 19.7 percent), and slightly lower payment rates after insurance collection (36.7 percent 38.7 percent). But outsourced RCMs took over 40 percent longer to recover payments from the self-insured or uninsured. They also had higher initial denial rates and higher denial write-offs, which translated into $22.7 million in lost revenue for the average 400-bed hospital. The study did not analyze the comparative costs of running in-house systems versus contracting them out (Crowe 2018).

These types of industry surveys are based on small sample sizes, and biases may emerge from how questions are framed. Nonetheless, they are consistent in reporting that RCM solutions have not delivered on the efficiencies promised by tech vendors and consultants. That has laid the groundwork for the new wave of enthusiasm for AI solutions in RCM systems.

Patient Experiences with RCM Companies

US hospitals have used outsourced RCM companies not only to improve billing efficiencies but to distance themselves from aggressive bill collecting. Non-profit hospitals are reluctant to aggressively pursue patients over unpaid bills, and few turn to lawsuits (Bannow 2019). But some evidence suggests that outsourced RCM companies have been more aggressive in bill collecting than hospitals.

Medical debt is a serious problem affecting roughly 17 million adults and 15 percent of households in the US in 2021. The total debt of $220 billion is disproportionately owed by people of color, women, those with low incomes or no health insurance, those with poor health or a disability, and those living in rural areas or the south (Rakshit et al 2024).

Some private equity-owned RCM companies have diversified into debt collection and medical payment products such as medical credit cards and medical loan services. Medical credit cards and interest-free loans are viewed as a way for patients to pay bills in installments, but they may leave them – sometimes unknowingly – with payments that are larger than they might have been able to negotiate with the hospital or insurance company. With medical credit cards, hospitals may receive payment up front from the billing company, which in turn pursues payments from the patient, who is at risk of facing hidden fees and large interest payments. Interest-free loans allow patients to pay for medical expenses by taking out a loan from the billing company, which places an additional fee on the hospital. While originally viewed as a means for patients to pay in installments, patients may feel pressured to sign these agreements *while in treatment* in hospitals and ER departments (Appelbaum and Batt 2020: 90-92; Fenne 2024).

Government-funded insurance prohibits patients from being required to pay as a condition of treatment (Luthra 2018; Rosato 2018). Hospitals may estimate the patient's cost in advance of treatment, taking insurance payments into account, but without a credit check to see if the patient can afford to pay as required by law. Patients who agree to the offer must pay the lender monthly for the full amount they have agreed to pay, even if it is more than what the patient would have owed after their insurance company negotiated with the hospital (Appelbaum and Batt 2020: 90-92). Lending data by the Consumer Financial Protection Bureau found that interest payments can inflate medical bills by almost 25 percent, while a report by IBISWorld estimated that the patient financing industry had profit margins of over 29 percent (Fenne 2024).

Complaints to the Federal Communications Commission (FCC) about aggressive tactics increased in the early 2010s. Between 2010 and 2014, for example, the government reported a dramatic 560 percent increase in the number of lawsuits claiming violations of the Telephone Consumer Protection Act (TCPA) by RCM and other bill collections companies. This led state and federal regulators to increase their scrutiny of RCM companies, and in December 2014 the Consumer Financial Protection Board (CFPB) held a public hearing to address the "unnecessary and frustrating challenges" faced by people who have medical bills (Kutscher 2015). Notably, RCMs must report any problems they have in collecting payments from patients to credit reporting agencies, and the resulting bad marks on a person's credit report may continue long after the overdue bills have been paid. In August 2015, the FCC ruled that the decades-old Telephone Consumer Protection Act (TCPA) applies to calls by bill collectors to cell phones, not just landlines. The FCC made clear that debt collectors must confirm express consent before autodialing a cellphone. They are allowed one wrong number call to a cell phone. Violations of the TCPA incur substantial financial penalties (Kutscher 2015). Finally, under the Biden

administration, the Consumer Financial Protection Bureau (CFPB) issued a rule prohibiting consumer reporting agencies from including medical debt information on credit reports and scores (CFPB 2025). But that doesn't prohibit RCM companies from pursuing debt collection, which disproportionately affects the most vulnerable.

Other private equity-owned RCM companies have been hit with large numbers of complaints filed with the CFPB. Between 2015 and 2021, for example, Transworld Systems Inc, the largest accounts receivable management services company in the US, was bought out by Platinum Equity in 2014, and recapitalized by Clearlake Capital Group in 2018. In that time, of the 6,819 complaints against the company, 1,859 (27.3 percent) were for aggressive medical debt collection (PESP 2021). TSI's website emphasizes its effectiveness in patient bill collecting, and its growing importance as out-of-pocket expenses are projected to continue escalating in the future (TSI 2025).

In sum, EHR systems provided the platforms for layering on a series of additional software programs to automate claims and financial management, and private equity firms accelerated their leveraged buyouts of RCM companies since the 2010s – using them to add on other types of medical debt payment products and debt collection as well as AI and machine learning applications. These companies lack transparency; no systematic data exists to assess the relative value creation versus value extraction from these systems. Healthcare organizations have become increasingly dependent on EHR-RCM systems embedded in their operations – and they are locked into such systems regardless of their deficiencies. These systems also facilitate 'efficient' billing and medical debt collection, and patients with high rates of medical debt due to economic or medical conditions may disproportionately pay the costs.

Data Analytics, Algorithmic Decision-Making, and AI

The current enthusiasm over artificial intelligence in healthcare is reminiscent of that for electronic medical records 50 years ago, but on steroids. AI applications have emerged much more quickly, using prior advances in data analytics and EHR platforms already in place. AI allows software systems to simulate problem-solving and decision-making while machine learning applies AI to systems to produce automatic learning. While the technology is unproven with many questions unanswered, healthcare organizations and insurance conglomerates are rapidly integrating AI into decision-making. They expect massive cost savings from labor-saving automation, but empirical evidence on this point is undeveloped.

In this section we review some of the available research and case studies that highlight the concerns of medical professionals, practitioners, and policymakers.

Three central problems are evident. First, the use of AI in healthcare is proceeding without regulatory safeguards. The hurried adoption and complexity of AI and machine learning make it

extremely difficult for lawmakers to catch up or come to agreement on how to regulate these rapidly changing technologies.

Second, while regulation lags far behind, financial actors and tech firms are moving in quickly to take advantage of profit-making opportunities, regardless of how AI applications affect patient care. As a professor of biostatistics and data science at Harvard University noted, there's "… a clear double standard in medicine: While health care institutions carefully scrutinize clinical trials, no such process is in place to test algorithms commonly used to guide care for millions of people" (Ross 2021a).

Third, data-driven decision-making is non-transparent, as assumptions are deeply buried in software systems or big data. This makes it extremely difficult to assess whether AI is being used for cost savings or cost shifting, better care quality or worse. In the two cases we present here, it took investigative reporters months and months of ploughing through hundreds of pages of documents and hundreds of interviews with employees and others to learn how algorithmic decision-making was being used. They found that cost savings for insurers and hospitals meant cost shifting to patients as well as delayed or denied patient care.

Venture capital, private equity, and Big Tech have financed a range of firms using data analytics, algorithms, and more recently artificial intelligence to drive cost management, risk management, decision support, 'value-based care enablement', and similar functionalities. Roughly 230 data analytics vendors in the PitchBook health IT database as of July 2024 have previous or current VC/PE backing – with some 75 currently backed by private equity and over half with current VC backing (PitchBook, author calculations). VC or PE firms typically provide initial financing, followed by PE buyouts to add on to other small firms and create larger tech vendors for strategic acquisitions by insurance or health services corporations.

Private equity firms, however, are also buying up more mature data assets. In January 2022, IBM announced that it would scrap its foray into healthcare artificial intelligence and sell off the core data assets of Watson Health. IBM had spent billions buying up health information companies to build an AI business providing information to pharmaceutical companies, hospitals, and private research firms. The database of 270 million Americans – almost 80 percent of the population – includes patient health records, medical images, and insurance claims. The private equity firm Francisco Partners bought out the company. IBM decided to scrap the venture after its products failed to deliver accurate predictions; for example, its Watson for Oncology garnered complaints from doctors around the world, and IBM's own medical experts cited "multiple examples of unsafe and incorrect treatment recommendations" (Ross 2022a).

Large Medicare Advantage (MA) insurers have become leading users of AI-driven decision-making. MA plans are essentially privatized Medicare – administered through large insurance corporations but paid for by Medicare. Once a senior enrolls in a plan, the MA insurer is responsible for covering all needed care, but most MA plans require members to use a narrow

list of in-network providers and to get pre-authorization before care is provided. As MA profit margins depend on finding ways to limit the cost of Medicare claims, MA plans have been particularly active in their use of AI-driven decision-making tools. And their impact on older Americans is large, because over half of all Medicare-eligible seniors are enrolled in MA programs as of 2023. The largest three MA insurers, with almost 80 percent of the market, are United Health Group, Humana, and CVS Aetna.

According to a recent investigation, "The predictions have become so integral to Medicare Advantage that insurers themselves have started acquiring the makers of the most widely used tools. Elevance, Cigna, and CVS Health, which owns insurance giant Aetna, have all purchased these capabilities in recent years. One of the biggest and most controversial companies behind these models, NaviHealth, is now owned by UnitedHealth Group (Ross and Herman 2023a)."

Concern over AI-driven decision-making tools has been growing. Research in biomedical informatics has begun to identify how and why AI may produce inaccurate predictions. A 2021 study of Epic's AI algorithms found that they were delivering inaccurate information on seriously ill patients. Epic is the largest and most powerful actor in the market for selling algorithms, as they work inside its EHR system – which as of 2021 contained an estimated 250 million records. It is the dominant platform adopted in large hospital systems and Academic Medical Centers (AMCs). The investigation was based on dozens of interviews with data scientists as well as Epic's clients from several healthcare systems and their employees. It found that Epic has paid health systems up to $1 million in cash incentives to adopt its own or other predictive algorithms. Of particular concern was Epic's algorithm for predicting sepsis, a life-threatening infection. In many hospitals that tested Epic's sepsis algorithm, it did not reach the company's advertised accuracy rates of 0.76 to 0.83, resulting in missed cases and high rates of false alarms. Employees in client hospitals said that the algorithm "… routinely fails to identify the condition in advance and triggers frequent false alarms" (Ross 2021b). At the time, Epic had developed some 20 predictive algorithms, but some independent evaluations also found limitations in their ability to predict patients' length of stay or likelihood of becoming seriously ill (Singh 2021).

Another 2021 study by medical researchers at Chicago Booth's Center for Applied Artificial Intelligence found systematic racial and economic bias in the routine use of algorithms for decision-making in healthcare organizations, insurers, and other related businesses. They found racial bias arises because algorithms are often 'trained' using data from a White population, so they do not accurately predict outcomes for Black patients. Examples of 'high' risk of bias included algorithms used to triage patients in emergency rooms, predict likely onset of disease for preventative care, and identifying additional services needed for patients, with fewer resources going to Black patients. They also found, "… enormous racial bias in cost-prediction algorithms" (Obermeyer et al. 2021).

MIT researchers in collaboration with STAT journalists examined the question of whether popular algorithms used to warn of bad outcomes for patients hold up over time. They do not; instead, they found that "…subtle shifts in data fed into popular health care algorithms — used to warn caregivers of impending medical crises — can cause their accuracy to plummet over time, raising the prospect AI could do more harm than good in many hospitals… the algorithms deteriorated over several years, delivering faulty advice about which patients were at the highest risk of deadly complications and prolonged hospital stays." Even when the algorithm was trained and tested on data from a single hospital system – which should produce higher accuracy – the researchers found that the accuracy still declined, what they referred to as dataset drift. Spurious correlations are also worrisome because, "As the real-world context around an algorithm changes, so does the relationship among the data variables it uses to find patterns and make conclusions" (Ross 2022b).

In 2022, the Center for Medicare Advocacy (CMA) specifically examined the extent to which AI tools are used for Medicare programs, and the extent to which they supplant rather than supplement decisions for prior authorization of treatment, post-acute care, or admission and discharge planning. It highlighted one specific problem: because the AI-powered tools are proprietary, they are unregulated and non-transparent, preventing public knowledge of how they work. Medicare rules only allow them to be used for recommendations, and MA insurers and other users claim that is what they do. But increasing evidence shows otherwise – that in practice, users often substitute them for clinical or medical decisions without a critical assessment of their impact on patients (CMA 2022).

The abuse of algorithmic analytics and AI decision tools for financial gain has been documented in a series of explosive investigative reports since 2022. Below, we describe two examples. The first, NaviHealth, formerly owned by private equity firms and acquired by United Health Group (UHG) in 2020, has been the subject of a series of exposes by *STAT News* reporters Casey Ross and Bob Herman. The second firm, Multiplan, also built through PE leveraged buyouts, was investigated by *New York Times* reporter Chris Hamby. The studies are thoroughly researched and replete with stories of how patients have borne the costs – both financially and in terms of care delayed or denied. Both corporations have been under Congressional investigation and have numerous lawsuits filed against them, which are still pending in 2025.

NaviHealth

NaviHealth began in 2011 as a technology and data analytics firm, providing tools to help hospitals and insurance plans save on Medicare claims and reduce post-acute care readmissions. It quickly gained large health systems and insurance clients like HCA, Community Health Systems, and Cigna. It was founded by Tom Scully, a partner of the private equity firm Welsh, Carson, Anderson, and Stowe (WCAS). He was the associate director of the Office of

Management and Budget under the George H.W. Bush administration, became the CEO of the Federation of American Hospitals, the trade association for the investor-owned hospital sector (1995-2001), and then served as Administrator for CMS under George W. Bush (2001-2004). For over 20 years he worked tirelessly to privatize Medicare, and played a pivotal role in creating Medicare Advantage under the George W. Bush administration (Dayen 2023)

As a partner at WCAS, Scully started NaviHealth with $7 million of his own money – plus about $50 million from WCAS and other wealthy friends – to buy out a small data analytics firm with an algorithm using patients' health records to predict their post-acute care length of stay and discharge date. He marketed the product to insurance plans, and by 2015 NaviHealth's insurance contracts covered two million people (Ross and Herman 2023a). He sold it to multinational health products distributor Cardinal Health for $410 million for an eight-fold return on investment. A year later, Cardinal flipped the company to private equity firm Clayton, Dubilier, & Rice in a leveraged buyout worth $650 million. In 2020, Cardinal sold it for $2.95 billion to Optum Inc., the United Health Group subsidiary that includes technology and data analytics services (PitchBook 2024a). While these financial firms were making billions, they were violating wage and hour laws by classifying non-management workers as exempt from overtime pay, resulting in a $4.7 million settlement – a tiny fraction of what they had made through financial engineering (Tornone 2020).

Ross and Herman's investigation was based on interviews with people and patients with direct experience with NaviHealth, industry insiders, and healthcare industry actors, including insurance executives, policy experts, physicians, and patients. They reviewed 'hundreds of pages' of corporate documents, federal records, and court filings. NaviHealth is also used by UHG's major competitor, Humana. Medicare Advantage plans were using "unregulated predictive algorithms under the guise of scientific rigor, to pinpoint the precise moment when they can plausibly cut off payment for an older patient's treatment" (Ross and Herman 2023a). This would cause major disputes between doctors and insurers that led to delayed treatment of elderly patients, often seriously ill or facing life-threatening conditions, and require patients to appeal the decisions, leading to further delays. Between 2020 and 2022, the number of appeals filed to challenge MA denials increased by 58 percent to 150,000, according to CMS data – a count that fails to include thousands of patients who never appealed negative decisions. Most denials are overturned (Ross and Herman 2023a).

Ross and Herman's further investigation into UHG revealed internal documents plus multiple employee testimonials saying that they were required to follow the projections from the data system. Case managers said the company set strict performance goals requiring them to keep patient rehab stays within one percent of the days projected by the algorithm, under penalty of discipline. Their stories and those of many patients capture the extent of damage to patients – of seniors sent home before fully healing or having to pay out-of-pocket for care that was denied. In the meantime, a 2022 corporate report stated that NaviHealth had achieved average savings of

more than 20 percent per episode of care – an estimated savings of several hundred million dollars annually (Ross and Herman 2023b).

In April 2023, the federal government announced regulations stipulating that MA plans could not reject coverage of tests, procedures, drugs or supplies that would normally be covered under traditional Medicare (Herman 2023). In May 2023, the Senate opened hearings into Medicare Advantage denials, requiring UHG, Humana, and CVS/Aetna to provide internal documents on their decision-making processes for claims and their use of AI (Herman and Ross 2023a). In November of that year, patients filed a class action lawsuit alleging that UHG used software algorithms to 'systematically deny claims' of its Medicare Advantage enrollees. The suit also claimed that UHG knew the algorithms had an extremely high error rate based on the percentage of denials that were subsequently reversed through appeals (Ross and Herman 2023b).

In December Herman and Ross provided additional evidence from internal company documents and employee interviews that UHG used prior authorization rules to restrict access to rehab therapy to specific groups of seriously ill patients in nursing homes or suffering from cognitive impairment. They were routed for 'quick denial' without apparent clinical justification or the knowledge of their doctors or the patients. Those rules were suddenly reversed in November 2023 (Herman and Ross 2023c). In May 2024, UHG sought to dismiss the class action suit, arguing that the patients should first exhaust the CMS appeals process. The plaintiff families argue that the current CMS appeals process would take years for remedies (Herman and Ross 2024).

In the meantime, longstanding NaviHealth CEO Harrison Frist stepped down. He is the son of former Senate Majority Leader Bill Frist, who under the George W. Bush administration helped craft the Medicare Advantage law. Bill Frist, in turn, was the son of Thomas Frist Sr., who founded Hospital Corporation of America, the largest investor-owned healthcare system in the country. To distance itself from negative reputational effects, UHG has rebranded NaviHealth as 'Home & Community Care' (Herman and Ross 2024).

Multiplan

Multiplan is another data analytics firm that contracts with large insurance corporations to help them with cost management. According to the 2024 *New York Times* investigation, its 'cost recommendations' software has allowed insurers to make millions and employers to pay less while reducing payments to physicians and other healthcare providers and shifting costs to patients. It found that patients were hit with unexpectedly high bills that led them to delay care or end long-term care. For this report, The *Times* interviewed more than 100 patients, billing specialists, doctors, health plan advisers, and former MultiPlan employees. It reviewed more than

50,000 pages of confidential corporate records, claims information, legal filings, and other documents (Hamby 2024a).

Founded in 1980, MultiPlan Corp. has grown into a leading technology platform that provides out-of-network cost management, payment and revenue integrity, data and decision science, business-to-business (B2B) healthcare payments, and other services (Multiplan Form 10-K 2024). Most of MultiPlan's revenue comes from fees for use of its payment recommendation system for out-of-network healthcare service, provided through its repricing algorithm, Data iSight (Pitchbook 2024b). The company initially determined payments primarily through negotiations with insurers, offering modest discounts in exchange for agreements not to collect more from patients.

In 2006, founder Donald Rubin sold the company to a private equity consortium led by the Carlyle Group – investing $200 million in equity (20 percent) for a $1.04 billion buyout. The Carlyle Group began more aggressive pricing practices and used Multiplan as a platform for a series of leveraged buyouts of other data analytics vendors before flipping it in 2010 to PE firms BC Partners and Silver Lake for $3 billion. BC and Silver Lake refinanced Multiplan's large debt overhang three times before taking a $750 million dividend recapitalization for themselves and investors. In March 2014, they flipped it again to another consortium of PE firms for $4.4 billion (with 75 percent debt financing). Two years later, in June 2016, the PE consortium sold Multiplan to another PE consortium for $7.5 billion using 63 percent debt. In 2017, the consortium took out another dividend recapitalization to award itself and investors $1.3 billion in dividends. The company went public in 2020 through a reverse merger with Churchill Capital Corp III, an operator of blank check companies (Pitchbook 2024e).

By 2019, major insurance companies such as UnitedHealthcare, Cigna, and Aetna were using MultiPlan's services. While private equity firms were making billions in leveraged buyouts of Multiplan, the company was making its money by using data analytics to save insurance companies money and shift costs to patients. MultiPlan's software is used to service employer 'self-funded' insurance plans, which now cover most Americans. While fees for 'in-network' physicians and hospitals are preset, those for out-of-network providers are not. Employers contract with insurance companies that use Multiplan to calculate what they should pay for out-of-network services, and Multiplan typically recommends that the employer pay less than what the provider has billed.

The calculation takes the amount a doctor charges, subtracts MultiPlan's recommended payout, and identifies the resulting savings or discounts. Typically, both MultiPlan and the insurer collect a percentage of the declared savings as a processing fee. This system enables insurers to profit by reducing medical bills and charging employers for some of the savings – without underpaying providers to the point where they would sue (Hamby 2024a).

Data iSight is MultiPlan's algorithm-based analytics software that makes the price recommendations. It uses data submitted by medical facilities to the federal government and techniques developed by Medicare to estimate treatment costs, adding a profit margin. MultiPlan claims that it applies multipliers to ensure fair profits for hospitals and reasonable market rates for physicians, but documents show that MultiPlan allows insurers to cap prices and set what they consider to be fair profit margins for medical facilities. While Data iSight starts with Medicare's rate-setting methods, subsequent calculations are less transparent.

As a result of Multiplan's algorithmic recommendations, providers receive lower payments, and patients absorb the unpaid portion of the bill, which is higher due to Multiplan's cost recommendations. Former employees at MultiPlan reported that the company was completely 'numbers driven,' and that their bonuses were tied to 'locking in unreasonably low payments' for providers. In some cases, insurance companies receive fees for processing a claim that far exceeds the amount paid to providers who treated the patient. For example, in a lawsuit against Cigna, court records showed that Cigna received nearly $4.47 million from employers for processing claims from addiction treatment centers. The centers only received $2.56 million, while MultiPlan took $1.22 million (Hamby 2024a).

The relationship between insurers and MultiPlan has led to predatory billing practices for patients. Low reimbursement rates have burdened patients with unexpectedly large bills, reduced pay for doctors and other medical professionals, and left employers who fund health plans with high, often unanticipated fees. Meanwhile, the largest health insurance companies in the country have made substantial profits. In recent years, UnitedHealthcare, the nation's largest insurer by revenue, has gained approximately $1 billion annually in fees from out-of-network savings programs, including its collaboration with MultiPlan. In 2023 alone, MultiPlan identified nearly $23 billion in bills from various insurers that it recommended not be paid (Hamby 2024a).

Lack of transparency and regulatory oversight have allowed these types of financial schemes to continue. Employer-funded health plans are mostly exempt from state regulations. And federal enforcement, which is housed within the US Department of Labor, is crippled by the lack of resources, with one investigator for every 8,800 health plans (Adams 2024).

Victims of predatory billing practices have had to turn to the courts to seek relief. Recently, MultiPlan has been hit with multiple allegations under the False Claims Act, with whistleblowers and government entities accusing it of schemes that resulted in fraudulent billing and underpayment practices. These often involve collaboration with major insurers to use data analytics and pricing tools to underpay healthcare providers. Over a dozen lawsuits have been filed between 2017 and 2024 alleging anticompetitive behavior and collusion with major insurers – including UHG, Cigna, and Aetna – to fix prices and lower payments to providers (Adams 2024; Bell 2024; Hamby 2024b, Muoio 2024a).

In sum, the problems of using data analytics, AI and algorithmic decision-making in healthcare have begun to emerge through medical research and investigative reporting. Their use is unregulated, with no independent process to scrutinize them before they are used in healthcare systems and no guardrails against potential downside risks for patients. They are non-transparent, making it extremely difficult to assess whether AI is being used for cost saving or cost-shifting from insurers or healthcare systems to employees or patients. And early research has identified several major concerns over algorithmic and AI-driven decision-making systems. These include the inaccuracy of data that AI uses, leading to improper diagnoses or care recommendations; racial and economic bias embedded in AI systems; the use of AI 'recommendations' as strict rules to be implemented; and the hidden ways that data analytics may be used to shift costs from hospitals and insurance companies to healthcare providers and patients. In the meantime, Wall Street, Silicon Valley, and Big Tech actors are making billions selling data and AI systems that lack sufficient testing, transparency, or regulation.

Monetizing Patient Health Data

Over the past several decades, a multibillion-dollar industry of buying and selling patient health data, referred to as 'secondary data,' has emerged. The EHR secondary patient data market is highly lucrative because the data is valuable for marketing, data analytics, private corporate research and biomedical research. It is cross-sectional, longitudinal, and comprehensive – and it includes a patient's demographic information, medical and family history, vital signs, allergies, medications, diagnoses, hospitalization history, administrative and billing data, insurance information, immunization dates, radiological images, laboratory test results, and free-text physician notes. It also can be aggregated, formatted, and available for 'big data' machine-learning.

Federal laws and regulations have facilitated the emergence of this industry. Medicare increased the demand for insurance claims data and outside data processing firms. The Texas firm Electronic Data Systems (EDS), founded by former IBM salesman Ross Perot in 1962, won contracts from state Medicare and Medicaid programs, and 20 years later it was acquired by GE for $2.5 billion. Medicare also awarded grants and sent hundreds of thousands of de-identified Medicare patient records to university researchers to develop data-mining techniques for insurance claims (Tanner 2016: 67-68).

From the 1990s on, Congressional passage of the HIPAA, HITECH, and ACA laws shaped the patient data market. HIPAA required protection of individual privacy, which became an industry norm, but privacy protections were limited. Healthcare providers and insurers (covered entities) that electronically transmitted data were required to protect patients' privacy. Healthcare providers included physicians or other providers such as psychologists, dentists, nursing homes, and pharmacies. They could share it with 'business associates' that provided related services and

were also covered by privacy mandates. Business associates include consultants, attorneys for healthcare providers, freelance medical transcriptionists, accounting firms that provide services to a healthcare provider, third-party claims processors, pharmacy benefits managers, and healthcare clearinghouses that translate claims from non-standard formats to standard formats. Thus, under HIPAA, a large number of healthcare and non-healthcare businesses have access to sensitive patient data such as mental health records. This information may be used for medical research provided patients authorize its use – but in some cases, without authorization (U.S. HHS 2024).

Moreover – and most importantly for the data mining and ad agencies – the law allowed any entity to have access to patient data provided it was de-identified, thereby legitimizing the monetization of patient data. As most healthcare providers had not adopted electronic systems in the 1990s, and as the data collected was limited to specific records of doctor-patient interactions, the amount of patient data available for monetization was limited. But as computer capacity and digitization expanded, fuller patient health histories were added to electronic records, and that information was aggregated for the secondary market – while the HIPAA rules remained unchanged.

Once the data is stripped of basic personal information (name, address, Social Security number), it may be sold. Pharmacy chains, pharmacy benefits managers (PBMs), hospital systems, physicians, insurance companies, and EHR vendors all collect, aggregate, and sell their data directly to pharmaceutical or other companies, or to research and marketing firms that act as intermediaries in the market. Many non-profit healthcare systems have set up for-profit subsidiaries for these purposes. Many doctors and most patients are not aware that their data is being bought and sold, but it is perfectly legal to do so.

While the HITECH law increased penalties for privacy and security breaches, it also mandated that all healthcare providers must collect this data, and that all patients must agree to the HIPAA rules if they want to receive care from any healthcare provider they see. And by throwing billions of dollars into EHR adoption, the HITECH Act dramatically increased the amount of EHR data available to be monetized. The ACA further contributed to the secondary data industry by mandating EHR systems for individuals who opted into the new local insurance exchange markets. As a result, an ever-larger swath of Americans –and a larger amount of health information in their personal records – became available for monetization.

Industry Evolution

Today’s billion-dollar industry of buying, selling, and mining patient data has its origins in the drug marketing agencies that emerged just after World II. In *Our Bodies, Our Data* (2016), Adam Tanner presents a thoroughly researched account of the industry’s evolution over 75 years.

It grew out of the 1940s Madison Avenue advertising world, where sophisticated marketing techniques were adapted to drug promotion by 'med men' like psychiatrist Arthur Sackler, who is credited with revolutionizing the sale of drugs to doctors. Sackler hooked up with Bill Frohlich, a German immigrant with his own ad agency, to 'coordinate' drug marketing contracts. In 1954, Frohlich founded Intercontinental Medical Statistics (IMS), tapping colleague David Dubow to run the business with Sackler's financial backing (Tanner 2016 23-29). In a 1980 interview with *Forbes*, CEO Dubow described the company as 'hyper profitable', with 20 percent annual growth rates over the prior decade and operations in 42 countries (Tanner 2016:30). IMS has dominated the medical data mining market since the 1950s and today monetizes billions of patient medical records each year.

In the 1970s and 1980s, other competitors entered the market, and data mining and marketing companies increasingly portrayed themselves as scientific research companies and downplayed their sale of data for marketing. New competitors often hired away IMS executives to launch their data businesses, such as drug wholesaler McKesson Corporation, which set up a pharma data services (PDS) subsidiary to aggregate millions of claims data. It surveyed hundreds of thousands of doctors, paying them $2-$10 per survey, and used the data to rank doctors according to which drugs they prescribed so they could better target them. The next step was to link individual doctors to prescription records, which representatives from PDS, IMS, and others did by convincing the American Medical Association to sell them individual doctor profiles from its Physician Masterfile. Unbeknownst to doctors, drug company sales reps then used doctor-identified data to target the biggest prescribers or to target certain doctors for specific and costly new drugs. The explosion of data from insurance claims, pharmacies, and middlemen made the data mining companies more necessary than ever to big pharma companies, which paid in the range of $10-$40 million for a full suite of IMS data and consulting (Tanner 2016:28-38).

At the same time that data mining and marketing agencies were entering the patient data market, tech vendors like Epic and Cerner were experimenting with digitalization of medical records. They were developing on a separate but parallel track – focused not on selling data to drug companies but selling electronic records systems to hospitals and physicians who aspired to reduce administrative costs. But the two tracks began to converge after passage of HIPAA, which clarified privacy rules. This facilitated the direction that the data miners were already moving towards – the integration of patient medical records into doctor-identified drug prescription data.

Over the next two decades, many large EHR vendors, insurance, and healthcare corporations – the 'covered entities' under HIPAA with access to millions of patient records – entered the patient data marketing industry by creating or acquiring subsidiaries to monetize de-identified patient data. Epic had a history of avoiding the data market, but now mines some 300 million patient records through its Cosmos system (Joseph 2023). Cerner permits customers to conduct analyses on its 150 million patient records in the form of 'data enclaves.' Large non-profit

hospital systems like Ascension and Mayo Clinic have partnerships with Google, where they provide access to their high-quality data. Kaiser Permanente and Geisinger Health also use the data they collect as an additional revenue stream to support their bottom line. Other big tech corporations like IBM have purchased healthcare businesses to gain access to this data. It entered the EHR data business by acquiring three firms with a combined total of 310 million patient records. More recently, the new interoperability rules put in place by CMS under the 21st Century Security Act allow patients data from devices like FitBit to be integrated into patients' EHR data. Google recently acquired Fitbit, with 28 million users (Enriquez-Sarano 2020: 2325-6, 2343).

Throughout the evolution of the industry, companies have portrayed themselves as contributing data for scientific purposes and the public good, while downplaying their use of it to make billions through marketing. And it is impossible to sort out how much data is used for marketing versus medical research or population health management. Healthcare systems like Kaiser Permanente emphasize their use of their own patient data for population health purposes. As the CIO of Kaiser noted shortly after passage of the HITECH Act, "For example, we are able to follow decades of data on diabetes patients," he said. "We can truly change the medical outcomes" (Freudenheim 2012).

There is also great enthusiasm in public health and medical research communities for the use of big data to advance scientific research. These have been limited, however, by the failure of EHR vendors to develop interoperable standards. Thus, data from Epic systems, as large as that data is, contains biases built into the type of patients that AMCs serve.

A more troubling concern is that HIPAA created two distinct sets of rules for medical research. Academic researchers are governed by traditional safeguards of medical ethics that include IRB (Institutional Review Board) oversight, peer review, and publication for the benefit of the scientific community and public health. But 'BigMedTech' firms – EHR vendors, insurance corporations, big pharma, and Big Tech firms – are not. Corporate control of the data market makes it less available for academics and other scientists, who lack the resources to purchase the data. As a result, private research companies are making use of the data and publishing results, but these are not subject to the ethical strictures that govern traditional clinical studies using identifiable patient data. As legal scholar Enriquez-Sarano notes,

"*The Privacy Regime has radically changed medical research regulation. Traditional clinical trials and retrospective studies are governed by the familiar safeguards of medical ethics including IRB review, peer review, and publication. But under the Privacy Regime, private-sector EHR-based studies are not subject to any ethical review"* (Enriquez-Sarano 2020:2319).

Private sector EHR research is unregulated, vulnerable to bias, and unpublished, according to legal scholar Enriquez-Sarano: "The risk that unpublished for-profit medical research promulgates bad science is real" (2020:2319). Studies that use this data may be valuable, but

because there is no transparency and the data are proprietary, they cannot be replicated. Data scientists working in for-profit settings typically lack the clinical or ethical training or professional constraints that academic medical scientists face, yet they have much more access to immense data sets. BigMedTech data dwarfs the amount of data collected in AMCs. And academic researchers also do not have access to the data because it is too costly. De-identification is costly and complex, requiring the processing of structured and unstructured (notes, text) into a standardized form, and often requiring machine-learning of natural language processing. (Enriquez-Sarano 2020: 2344-2350).

The asymmetric access to EHR data by private research firms over academic scientists is particularly worrisome, as the industry appears to be rapidly moving into the use of this data for AI and machine learning research and applications – again with few guardrails or oversight.

The Fight for Patient Privacy Rights

The sensitive issue of patients' privacy, who 'owns' the data, and whether corporations must get patients' consent to use it have dogged the industry from the beginning. But the amount of person-specific data exploded in the 1990s, with an increase in the number of fields collected, the specificity of the data, and the opportunity to collect more data (Zayatz et al. 2001). Given this expansion, coupled with passage of HIPAA, the debate over patient privacy versus data access for research and marketing became more salient among healthcare professionals, researchers, patient rights activists, and industry actors. Congress believed it had solved the problem of privacy with the HIPAA provisions, but patients' rights activists and advocates disagreed.

One of the early patient's rights leaders was Deborah Peel, a physician and psychoanalyst whose deep concern over privacy issues grew out of her own practice. She was Chief of Psychiatry at Austin's Brackenridge Hospital in 1979 and began speaking out on mental health issues. In the 1990s she was briefing legislators in Texas and then D.C. on the role of middlemen and corporate practices in mishandling patient data (Tanner 2016:78). She grounds her EHR arguments in the Hippocratic Oath, which requires doctors to keep communications with patients private so that patients feel free to reveal the kind of sensitive information needed for correct diagnosis and medical care. She views privacy as a constitutional and human right that HIPAA violates.

In 2004, she founded the non-profit organization Patient Privacy Rights (PPR) in response to the publication of the final rules governing HIPAA published in 2002. According to the PPR website, those rules "… eliminate patients' rights to control the use of personal health information. The right of consent was replaced with 'regulatory permission for covered entities to use and disclose health records for treatment, payment, and healthcare operations.' The federal

government put data holding institutions in control of the use, disclosure, and sale of patients' health information, from DNA to diagnoses to prescription records."

In 2006, she helped found the bipartisan Coalition for Patient Privacy, which includes over 50 national organizations representing 10.3 million people. The coalition worked to add new privacy and security protections to HITECH, which included "a ban on sales of protected health information (PHI) without consent, a list of all disclosures of health data from electronic health records systems, the ability to separate sensitive health data and prevent it from being disclosed, receive notice of data breaches, a new right to block disclosure of PHI for healthcare operations if you pay for treatment out-of-pocket, and requiring data to be encrypted" (Patient Privacy Rights N.D.).

During this period, several states were considering laws to improve privacy or curb the use of doctor-identified information by drug sales reps to push doctors to prescribe higher-profit new drugs when older generic drugs would suffice (Scott 1999). In June 2006, the New Hampshire legislature passed the Prescription Information Confidentiality Act, the first of its kind in the country, prohibiting the sale of information about physicians' prescribing practices for use in prescription drug marketing (Kasprak 2008). It did not prohibit these activities for data identified by zip code, geographic region, or medical specialty. Maine and Vermont passed similar laws in 2007.

IMS and other competitor data mining companies Verispan and Source International sued in federal court, arguing that the law violated their constitutional right to commercial free speech. The AMA sided with the data miners, as it makes millions selling its Physician Masterfile of 1.4 million doctors and medical students (Tanner 2016:55). The federal district court in New Hampshire ruled in favor of the data mining companies, but a US Appeals Court overturned that decision, arguing that the law does not regulate speech, but data transfers whose social benefits "pale in comparison to the negative externalities produced." The Maine court decisions followed this pattern (Kasprak 2008:2). The opposite occurred in Vermont, and the state appealed the decision to the Supreme Court, which supported the appeals court ruling that the law unconstitutionally burdened the speech of pharma marketers and data miners (Sorrell v. IMS Health, Inc., 564 U.S. 552 (2011)). The decision turned on the fact that the law barred the pharmaceutical actors but not researchers from doctor-identified data (Tanner 2016:57).

Under Peel's leadership, Patient Privacy Rights played an instrumental role in the development and passage of HB 300, a Texas bill setting a high bar for protecting medical data. The landmark legislation protects Texans' health data by banning the for-profit sale of personal health information and toughening the privacy laws about personal medical records. In 2012, Patient Privacy Rights introduced the Privacy Trust Framework, which is a set of 75+ auditable criteria that measure how much technology protects data privacy. It offers healthcare consumers the

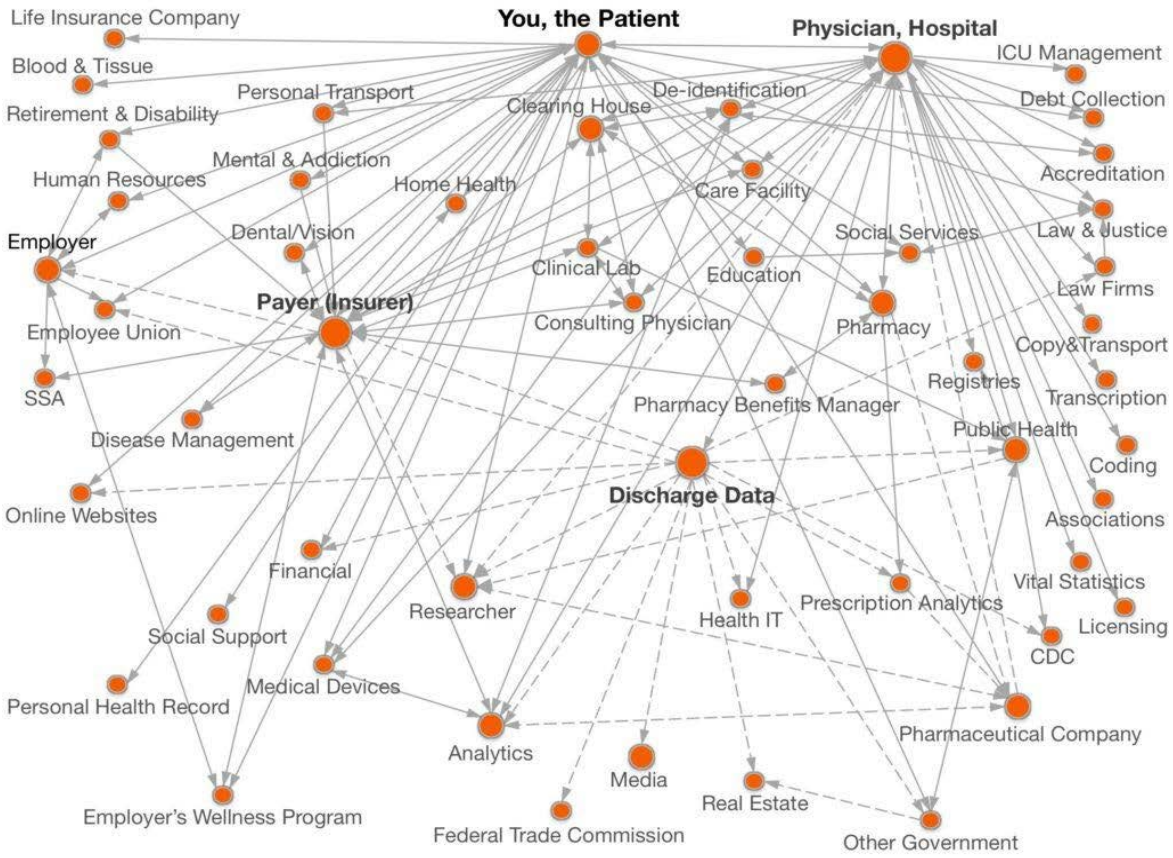
ability to control their most sensitive and sacred personal information by empowering them to make meaningful choices about health IT systems and products (Patients Privacy Rights N.D.)

Data Re-identification

While federal authorities and industry actors believed that HIPAA had solved the privacy problem by requiring de-identification when aggregated data is used for research or marketing purposes, computer science scholars began to show that data re-identification was possible. In 1997, MIT PhD student Latanya Sweeney analyzed publicly available medical insurance records of state employees and their families that had been stripped of identifiers except for birth dates, gender, and home ZIP codes. With this information she identified Massachusetts Governor William Weld and calculated that with the information she had she could potentially identify 87.1 percent of all Americans (Tanner 2016:93). For over two decades since Sweeney's research at MIT, many studies using different data sets have replicated the original results, even after states have attempted to improve the robustness of their privacy protocols (Sweeney 2015). The availability of genomic data increases the risk of matching data to individuals and to family members (Humbert et. al 2015). Other research has exposed the extensive sharing of personal data to third parties via mobile apps without user knowledge (Zang et al 2015).

The question of re-identification has spawned an entire subfield of data science research and has fueled the ongoing debate over the extent to which de-identification sufficiently protects patient privacy. Sweeney has published extensively on this question and founded the Data Privacy Lab at Harvard, a program in the Institute for Quantitative Social Science (IQSS) focused on creating technologies and related policies for 'balanced, integrated solutions' to ensure privacy protection while also allowing private (or sensitive) information to be used for beneficial purposes. That group hosts 'theDataMap,' which identifies which entity has access to what kind of patient data (see Figure IV). Each solid line represents data that is personally identified, while dotted lines indicate de-identified data.

Figure IV



Source: theDataMap. https://thedatamap.org/index.php

On the website, viewers may click the organizational buttons to find out what types of data each organization has access to. The most complete patient information comes from state discharge databases (SDD), the largest circle on the map, followed by payers and hospital/physician providers. SDD is based on state-mandated reporting systems that require hospital discharge data, with 31 states also requiring ambulatory and ER reporting (NAHDO 2024). Payers include private insurers, government, self-insured employers, health maintenance organizations (HMO), and preferred provider organizations (PPO)).

In sum, in this section we have shown that passage of the HIPAA and HITECH Acts had the unintended consequences of facilitating the growth of a completely unregulated multibillion-dollar industry for marketing aggregated patient data. While HIPAA privacy rules were designed to protect individual patient data, they also allowed 'de-identified' (stripped of personal identifiers) to be used for secondary purposes, such as medical research or population health management. But large ad agencies and data mining companies that pre-dated HIPAA were well-positioned to take advantage of de-identified data and monetize it for marketing and private research.

Because de-identified data is costly and held by large EHR vendors, insurance corporations, and healthcare organizations, academic medical researchers often do not have access to it. Instead, it is sold to large data analytics and private research or pharmaceutical companies that do not have to follow traditional medical ethics standards and clinical protocols. Given the proprietary nature of the data, studies cannot be replicated; and it is unclear whether this research meets scientific standards or not. The complete lack of transparency means that the public cannot assess the extent to which patient data is being used for private gain versus the public good.

A related and ongoing concern is patients' privacy rights. As EHR platforms have become the basis for integrating end-to-end revenue cycle management, hundreds of actors now have access to patients' personal health information: The ecosystem of healthcare organizations, providers, insurers, tech vendors, and related businesses with access to personally identifiable information has grown substantially over time. Patients' rights advocates are particularly concerned about the extent to which sensitive mental health and other personal information can be accessed by entities without a clear 'need to know.' A related concern is that de-identified information may be re-identified, as shown in a growing number of empirical studies using advanced data analytic techniques.

Cybersecurity Risks from EHR Systems

The hyper accelerated changes in features and capabilities of IT systems and big data over the last three decades have regularly rendered obsolete the privacy and security regulations originally adopted in HIPAA and updated in the HITECH Act. As seen in prior sections of this report, this has led to ongoing problems in the privacy and security of patient data. Moreover, loopholes in the regulations, including the failure to include as 'covered entities' several types of vendors with access to personal identified data, has led to even greater exposure of personal records to privacy and security breaches. While the 21st Century Cures Act created incentives to enhance interoperability, it failed to update data privacy or security standards nor expand the coverage of HIPAA to a broader set of actors.

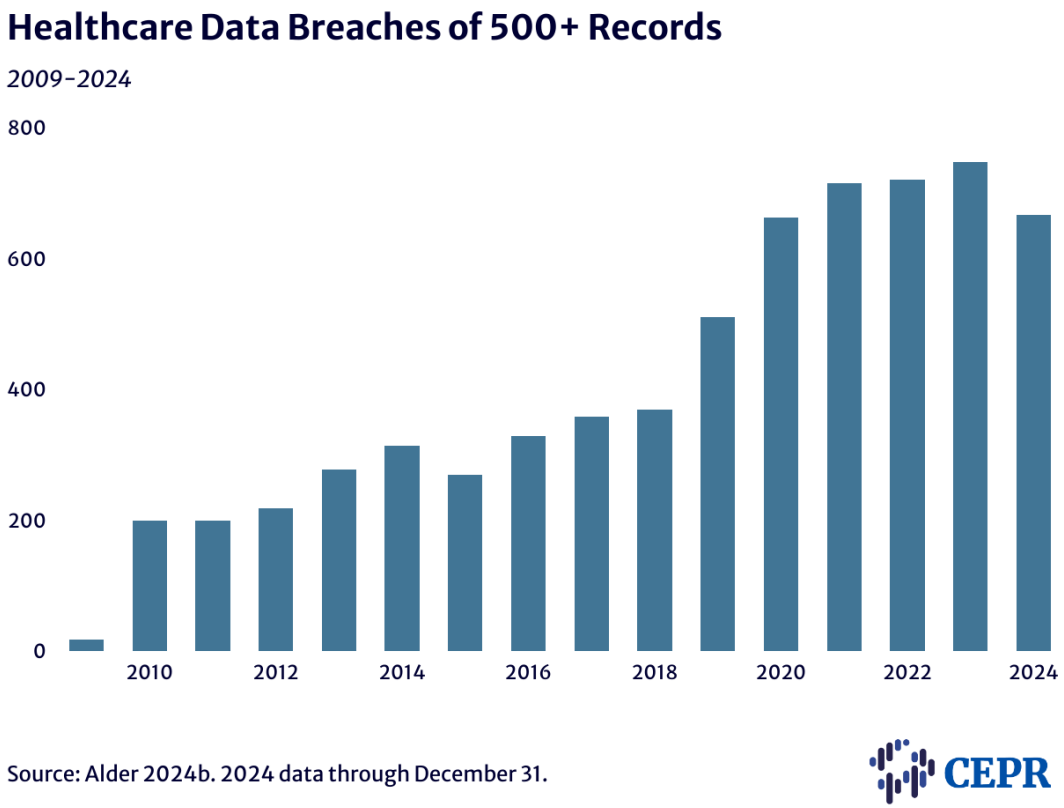
Healthcare has many more data breaches than any other sector of the economy because healthcare data is more valuable on the black market; it takes longer for healthcare breaches to be discovered, so that the data can be used longer. By contrast, stolen credit cards can be quickly blocked. Healthcare systems are also vulnerable because they are large, centralized vertically and horizontally integrated organizations that contain a vast array of sensitive patient information that healthcare providers need on a moment-to-moment basis. The integration of EHR, RCM, and other electronic records systems –coupled with the thousands of healthcare, payer, and related businesses with access to the data – means that its monetary value is much greater than that of other industries. John Riggi, former head of the FBI Cyber Division and Senior Advisor for Cybersecurity to the AHA, emphasizes that "The targeted data includes patients' protected

health information (PHI), financial information like credit card and bank account numbers, personally identifying information (PII) such as Social Security numbers, and intellectual property related to medical research and innovation" (Riggi 2024).

Since passage of the HITECH Act, healthcare data breaches have accelerated. The Office of Civil Rights (OCR/HHS) has been tracking data breaches affecting 500 records or more since 2009. Between then and the end of 2024, data breaches have affected some 748.5 million *individual* healthcare records (OCR/HHS 2024). *The HIPAA Journal* has aggregated these numbers into annual figures to assess trends over time. The number of individuals affected by healthcare security breaches was relatively low at 20 million or less between 2009 and 2018 (except for 2015), but climbed to 40 million in 2019 and 2020, 60 million in 2020 and 2021, hitting 160 million in 2023 and 180 million in 2024 – the latter due to the massive attacks on Change Healthcare and Ascencion (Alder 2024b)

Between October 2009 and December 2023, at the healthcare *organizational level*, 5,887 large healthcare data breaches were reported. Annual attacks held constant at between 200-400 annually until 2018, when the number surged to 747 by 2023 and 667 in 2024 (Figure V).

Figure V



The reasons for the breaches have changed over time. While loss and theft of records dominated the period from 2009-2015, those problems were reduced by widespread adoption of data encryption methods and better tracking methods. In 2024, most of the incidents involved hacking rather than ransomware, improper disposal, loss/theft, or unauthorized access (Alder 2024b).[2]

The severity of attacks also increased, with the number of individuals affected by breaches growing from about 10 million in the pre-2015 period to 140 million in 2023. Three massive data breaches in 2015 account for the 100 million people affected by breaches that year, including Anthem Inc. (78.8 million), Excellus, and Premera Blue Cross. The ransomware attack at Change Healthcare in February 2024 was the largest ever, affecting one in three Americans. OCR estimates that in the first half of 2024, about 120 million individuals have been affected by data breaches (U.S. HHS 405(d) N.D.)

Among the 60 largest attacks reported to OCR, Change Healthcare is by far the largest, followed by Anthem Inc. (78.8 million, 2015), American Medical Collection Agency (26 million, 2019), and Kaiser Foundation Health Plan (13.4 million, 2024). On June 21, 2024, Geisinger Healthcare suffered an attack that exposed 1.3 million records (OCR 2024). Overall, there are far more attacks targeted at healthcare providers than health plans or business associates, but the latter account for almost 40 percent of the individuals with breached records (Alder 2024b).

The fact that data security breaches are occurring in the largest healthcare systems that are supposed to have the most advanced EHR systems is noteworthy. For example, in 2023 HCA had 11 million records containing 27 million rows of data stolen from an external storage location used to format emails and posted online. HCA is the largest and most profitable healthcare system in the country, with 184 hospitals and 2,000 additional sites serving 31.2 million patient visits annually. A follow-on lawsuit alleged that HCA failed to take ‘reasonable security procedures and practices, like encrypting data or deleting it when no longer necessary’ and put patients at a ‘lifetime risk’ of identity theft (Olsen 2023). Another 2023 attack occurred at Johns Hopkins Health System in an attack by a Russian-linked Ransomware group through a vulnerability in its MOVEit file transfer software. Patients were not notified until more than six weeks after the breach (Halleman 2023a).

The size and complexity of consolidated healthcare systems also means that it often takes weeks for them to know how much data has been compromised. Ascension Healthcare – with 140 hospitals, 40 senior living facilities, and 123,000 employees – was hit with a data breach in early May 2024, leading to delays in elective surgery and the need to divert ambulances. Doctors had to switch to paper records. Due to its size and complexity – Ascension has 25,000 network servers – the hospital did not know how much data had been compromised even after several weeks of investigation (Muoio 2024b).

The financial costs of data breaches are high and growing, according to a 2023 IBM data security breach report (IBM 2023). For the US economy overall, the average cost of a breach was $4.45

million in 2023, an increase of 15.3 percent over 2020. The US has the highest cost of data breach of any other country or region in the study. Cloud environments were particularly vulnerable, with 82 percent of breaches involving data stored in the cloud, whether public, private, or multiple environments. This finding is noteworthy, as leading EHR vendors – including the number two market leader, Oracle Health – are shifting patient data to cloud environments (IBM 2023).

The cost of healthcare breaches is particularly staggering: For the 13thh year in a row, the healthcare sector reported the highest data breach costs, on average $10.9 million per incident in 2023. Since 2020 healthcare data breach costs have increased by 53.3 percent. By comparison, the financial sector had the next highest breach costs but were still about 50 percent of the costs in healthcare (IBM 2023). The costs may include data recovery, fixing systems or investing in major upgrades, penalty payments to the government under the security breach regulations, and negative reputational effects from being listed on OCR's 'Wall of Shame' (OCR 2024). Many healthcare organizations have paid a ransom in order to prevent a data leak, although that percentage has fallen in part due to better preparedness. Nonetheless, 30 percent of ransomware victims in healthcare paid ransoms in Q4 of 2023, at an average of $568,705 per incident (considerably lower than in the past). In 2023, ransomware attacks increasingly targeted smaller companies with an average of 231 employees. The costs of recovery are particularly onerous for small hospitals, physicians' offices, and other small service providers (Alder 2024b)

Healthcare data breaches pose not only large financial costs, but major threats to patient care, patient safety, and patient privacy. According to a 2024 IBM Healthcare Data Security Survey, 87 percent of medical data is held in electronic records. Thirty-two percent of respondents had experienced a ransomware attack in the last three years, and of those almost half had patient data affected, and 27 percent had negative effects on patient care. Thirty-four percent of respondents said they did not recover the patient data after the attack. Only 63 percent of those surveyed had a cybersecurity plan in place (Couey 2024).

A recent example is Lurie Children's Hospital in Chicago, which serves 239,000 children each year and suffered a network attack in January 2024. The non-profit hospital had to shut down its phone, email, and electronic systems for weeks while still accepting patients and providing care. It took until late May to fully recover. Affected were 775,000 electronic records that included names, addresses, Social Security numbers, telephone numbers, email addresses, driver's license numbers, birth dates, health plan details, dates of service, and medical information. The suits claimed that the hospital should have known of the system vulnerabilities and took about five months to start notifying patients of their compromised information (Olsen 2024a)

Several class action lawsuits have been filed following data breaches that threatened patient care and data privacy and security including Ascension, HCA, Johns Hopkins Medical Center, Lurie

Children's Hospital, and most recently, Change Healthcare (Olsen 2023, Halleman 2023a, Muoio 2024b, Vogel 2024).

Change Healthcare Ransomware Attack

The ransomware attack on Change Healthcare represents the largest and most disruptive attack on a critical US infrastructure in history. It illustrates how the lack of regulation of large tech and healthcare corporations has led to a shocking level of vulnerability in electronic health systems that hospitals and physicians are completely dependent on for providing care. Change Healthcare was founded as a revenue cycle management company with venture capital and private equity funding in 2004. It grew by consolidating a dozen start-ups with different financial service platforms and skirted federal antitrust oversight by acquiring companies too small to be investigated. It went through a series of leveraged buyouts, including one by Blackstone, and became the largest RCM vendor managing the records of one in three Americans by 2022. It is the largest clearinghouse in the country for claims management and financial services including revenue cycle management, payment accuracy, clinical decision support services, and customer engagement software. Its clients include payers, providers, third-party administrators, pharmacies, and health IT developers.

A DOJ antitrust lawsuit to stop the buyout of Change Healthcare by Optum/UHG failed. Eighteen months after the acquisition, while UHG claimed it was still 'working on' the old technologies at Change, the cyberattack hit. Six weeks after the attack of February 21, 2024, the American Medical Association surveyed 1,400 members: 36 percent reported a suspension in claims payments; 32 percent could not submit claims because insurance companies will only accept electronic billing; and 22 percent could not verify eligibility for benefits. A third of providers had switched to some mix of paper and electronic workarounds. Small physicians' practices were particularly affected financially: 80 percent lost revenue from unpaid claims; 85 percent had to commit additional staff time and resources to complete revenue cycle tasks; and 51 percent had lost revenue from the inability to charge patient co-pays or remaining obligations. As a result, "55% of respondents had to use personal funds to cover practice expenses, 44% were unable to purchase supplies, and 31% were unable to make payroll." Physicians commented, "SOOOO much overtime… cost me additional $50,000 in payroll," "estimated $100,000 in unexpected costs," "This crippled our brand new practice. I am keeping the lights on using personal funds." The comments also pointed to serious negative effects on patient care, including pain management for cancer patients, no access to lab orders, patients unable to get care due to delays in prior authorizations or ability to cover medical bills (AMA 2024).

How did this happen in a multibillion-dollar healthcare corporation – one of the largest in the country? When UHG offered $13 billion to acquire Change Healthcare in 2021, the American Hospital Association vehemently opposed it as anti-competitive. Hospitals were concerned that

the buyout would consolidate too much of the country's health data from Change Healthcare (a neutral third party) into one powerful owner (Paavola 2021). It turns out they were right. The DOJ brought a lawsuit to block the merger, but federal judge Carl Nichols, appointed by President Trump, ruled in favor of UHG and allowed the merger to proceed if Change divested one of its businesses – which it then sold to private equity firm TPG (Liss 2022).

To understand how financial actors have built Change Healthcare while extracting billions in the process, it is important to trace its roots to 2004. Change Healthcare began as Emdeon Corporation, launched as a revenue cycle management (RCM) company in 2004 with $100 million backing from venture capital firm Kleiner Perkins and private equity firm PCG Capital Partners. In 2006, it was acquired in a $1.2 billion buyout by General Atlantic, a large generalist investment firm, using 81 percent debt financing. In 2008, Kleiner Perkins and PCG sold their stake in the company to General Atlantic and two new investors, Hellman and Friedman and BlueCross BlueShield Venture Partners, for $575 million – almost six times their initial investment. The company launched an IPO in 2009. Between 2009 and 2011, it acquired seven IT companies to diversify its platform services, including electronic data conversion, information management services, management consulting for healthcare payer market, technology-enabled accounts receivable denial and recovery, and technology-enabled provider of government, healthcare audit and recovery services for the payer market, and a platform that provided government program eligibility and enrollment services.

In 2011, Blackstone took Emdeon private again in a leveraged buyout valued at $3 billion (Monegain 2011). When it tried to refinance $1.43 billion in debt, the S&P assigned the loan a 'BB-' credit rating and its $375 million senior unsecured note at 'CCC+.' S&P said the ratings reflected its 'highly leveraged' financial risk profile and its 'weak' business risk profile with debt calculated at 7X EBIDTA (Reuters 2012).

Nonetheless, in 2014 Emdeon acquired Change Healthcare, a price transparency company, and rebranded itself Change Healthcare. By then its systems covered some 700,000 physicians, 5,000 hospitals, 1,200 payers and processed an estimated 8.1 billion transactions. It acquired Altegra Health, a risk management company, for $910 million in cash in 2015 (Miliard 2015). A year later, McKesson Corporation acquired a 70 percent stake in Change Healthcare for $4.45 billion. The joint venture received $4.87 billion in debt in 2017 for cash payouts to Change Healthcare owners ($1.75 billion), payouts to McKesson ($1.25 billion), and the remainder to pay down Change Healthcare's debt (Pitchbook 2024c). In 2019, Change Healthcare completed an IPO worth $641 million. When its attempt to refinance $3.84 billion in 2020 failed, it sought a new owner. In January 2021, Optum/UHG offered $13 billion to buy it out, including $5 billion in debt. Blackstone exited in full (PitchBook 2024c).

When the CEO of UHG, Andrew Witty, testified before the House Energy and Commerce Committee and Subcommittee on Health in May 2024, he blamed the failure on Change

Healthcare's 'older technologies' that UHG was still upgrading after almost two years. Whether Change Healthcare under PE ownership had failed to sufficiently invest in upgrades is unclear, but the company was sitting on $5 billion in debt when UHG absorbed it. On February 12, 2024, the AlphV ransomware group used compromised credentials to remotely access the Change Healthcare's Citrix portal, an application for remote desktop access. The system did not have multifactor authentication (MFA) turned on, a routinely used security method that would have protected it against the malware attack. The hackers had access to the system for over a week before they struck on February 21, allowing them time to download millions of records.

Change immediately shut down over 100 of its systems, which prevented medical claims and electronic payouts from being processed. Portals for prior authorizations were disrupted, as were prescription processing, claims payments, clinical decision support systems, and more. Given that Change processes one in three medical records and some 15 billion healthcare transactions annually, millions of people were affected. As indicated in the AMA survey, the failure hit small providers particularly hard – they claimed lost millions of dollars in revenues – and patients suffered delays in prescriptions, needed care, and had to cover medications out of pocket (Rundle 2024). The VA notified 15 million veterans that their records may have been compromised (Southwick 2024). Over 50 lawsuits had been filed against Change Healthcare by April, and dozens more by July (Olsen 2024b).

Almost three months after the attack, Witty said the company still didn't know exactly how many records were exposed – but when pressed by the committee, admitted that 'maybe a third' of Americans were affected. Witty also didn't know why the server that was hacked did not have MFA protection. It appeared that after a year and a half of upgrading, UHG had not identified servers in which MFA was turned off. In April, UHG paid the hackers a ransom or $22 million in Bitcoin, but Witty could not confirm whether they had made copies of the data so that they could later post it on the internet (Energy and Commerce Committee, US Congress 2024). By July 2024, UHG estimated the costs associated with the cyberattack at $2.45 billion. While its second quarter net income was down 23 percent year over year, it was still a hefty $4.2 billion (Cass 2024).

Healthcare Cybersecurity Enforcement

The federal government's efforts to keep up with technological advances and data breaches have been well-intentioned but fall far short of what is needed. Under the Cybersecurity Act of 2015 (CSA Section 405), HHS established a 'Healthcare Industry Cybersecurity Task Force' to report to Congress on the cybersecurity risks in healthcare (U.S. HHS 2018). It established a public-private coordinating council to issue a series of reports on the current resiliency of the sector and best practices for managing threats and protecting patients (U.S. HHS 405(d). N.D.; U.S.HHS 2023a, 2023b).

It wasn't until April 2024 that the FTC issued final rules to expand coverage of the Health Breach Notification Rule (HBNR) to health apps and other direct-to-consumer health technologies designed to extract personal health records (PHR) for marketing and other purposes. For the first time, it requires entities not covered by HIPAA – including vendors of PHR, 'related entities', and third party service providers to these vendors and related parties – to comply with its notification rules. In the event of a breach of unsecured personally identifiable health data, they must notify individuals, the FTC, and, in some cases, the media. It also defines the content of what must be included in these notifications (FTC 2024a).

The Office of Civil Rights has increased its enforcement actions even as security breaches outpace these efforts. The penalties for HIPAA violations have increased in number from single digits until 2015 to double digits since then. Financial penalties were substantial for the three major cases in 2015 — $16 million for the Anthem breach, $6.85 million for Premera Blue Cross, and $5 million for Excellus Health Plan. Since then, a larger number of small financial penalties have been imposed on small healthcare organizations, signaling that they do not fall under the radar of enforcement actions. In total, OCR has collected $144 million in penalties from 142 healthcare organizations and related entities since 2008. In the same period, state attorneys general have captured $223 million in fines from 60 organizations while the FTC has recovered $42 million (Alder 2024b).

In 2023, the FTC also took action against companies violating the HBNR, including Easy Healthcare, GoodRx, and BetterHelp, Inc. Easy Healthcare assured users of its Premom ovulation tracker that their information was non-identifiable and for its use only, but nonetheless shared it with third party advertisers. It was fined only $100,000 and barred from further data sharing. GoodRx was fined $1.5 million for sharing user personal health information matched to medications with Facebook, Google, and others for targeted advertising (FTC 2024a). An online counseling platform BetterHelp also disclosed consumer health data to third-party advertisers and paid $7.8 million in refunds to customers (FTC 2024b).

Conclusions

In Part II of this report, we examined the extent to which electronic health records systems, mandated by the federal government and adopted by most healthcare organizations by the mid-2010s, created the infrastructure for the layering on additional IT applications and the use of patient data for financial gain. Since passage of the Affordable Care Act, the federal government has continued to push value-based care models that require healthcare organizations to adopt sophisticated financial management systems – which in turn has heightened market demand for RCM systems owned by legacy IT vendors, private equity, venture capital, and Big Tech firms.

We document how these firms have played leading roles in financing or buying up software companies in these niche markets and consolidating them into larger and more powerful market actors. Increasingly, healthcare organizations have outsourced their health IT infrastructure to companies owned and operated by these financial actors – paying billions without assurance that the systems will deliver what they promise and without regulatory oversight.

Many of the problems found in EHR systems, including inaccurate or outdated information, continued in the 2010s – but revenue cycle management systems were nonetheless layered on the EHR platforms. While EHRs led to better billing processes and internal communications, little or no research calculated the net economic effects that include the hidden costs of installing, maintaining, and upgrading systems – as well as hiring, training, and retraining the entire healthcare workforce as systems continually change. That problem continues with the current health IT integrated systems and increasingly automated information processing and decision systems.

The data analytics segment of health IT expanded rapidly in the 2010s. Again, tech vendors and their systems are virtually unregulated, with no independent process to scrutinize algorithmic decision systems before they are implemented, and no guardrails against potential downside risks for healthcare organizations, providers, employees, or patients. They are non-transparent, making it extremely difficult to assess whether AI is being used for cost saving or cost-shifting from insurers or healthcare systems to employees or patients. Our review of early research and investigative reporting identified several major concerns over algorithmic and AI-driven decision-making systems. These include the inaccuracy of data that AI uses, leading to improper diagnoses or care recommendations; racial and economic bias embedded in AI systems; the use of AI 'recommendations' as strict rules to be implemented; the hidden ways that data analytics may be used to shift costs from hospitals and insurance companies to healthcare providers and patients. The case studies of NaviHealth and Multiplan, which provide cost and claims management services for large insurance conglomerates, illustrate these problems.

Our analysis of the data mining industry explains how the federal rules under HIPAA had the unintended consequence of creating opportunities for legacy drug and healthcare ad agencies to expand their patient databases for marketing purposes and financial gain. HIPAA allowed electronic health records to be aggregated and sold if they were stripped (de-identified) of personal information. Even when the explosive growth of this industry became evident, Congress failed to amend the HITECH Act to regulate the commercial use of patient data, which court decisions backed as 'commercial free speech.' Governmental failure to act has led to an unregulated multibillion-dollar industry in monetizing patient data, often without patients or healthcare providers' knowledge. Moreover, because de-identified data is costly and held by large EHR vendors, insurance corporations, and healthcare organizations, it is often sold to financial actors who can pay – often large data analytics and private research or pharmaceutical companies, which do not have to follow traditional medical ethics standards and clinical

protocols. Given the proprietary nature of the data, studies cannot be replicated nor evaluated for whether they meet scientific standards or not. The lack of transparency means that the public cannot assess the extent to which patient data is being used for private gain versus the public good.

Concern over patients' privacy rights is greater than ever. End-to-end RCM systems allow patients' data to be accessed by hundreds of actors. The ecosystem of healthcare organizations, providers, insurers, tech vendors, and related businesses with access to personally identifiable information has grown substantially. Patients' sensitive mental health and other personal information can be accessed by entities without a clear 'need to know.' A related concern is that de-identified information may be re-identified, as shown in a growing number of empirical studies using advanced data analytic techniques.

Finally, the escalation of data breaches and cyber-attacks in recent years reached crisis proportions in 2024, with some one in three records of Americans exposed in the one data breach of Change Healthcare's system. Healthcare is by far the most vulnerable industry to cyberattacks due to the high value of sensitive information on the black market. For the 13th year in a row, the healthcare sector reported the highest data breach costs, on average $10.9 million per incident in 2023. Healthcare organizations must now invest billions more in cybersecurity systems owned and operated by venture capital, private equity, and Big Tech.

We conclude that the federal laws and regulations that have stimulated health IT adoption were successful in the narrow goal of adoption, but the follow-on consequences — some intended and some not – have led to consequential negative outcomes for healthcare organizations, providers, workers, and patients. Venture capital, private equity, health IT vendors, and Big Tech have been able to extract billions through their ownership of health IT systems. They are almost entirely unregulated, and no systematic monitoring or evaluation systems are in place to evaluate the impact of these financially driven systems on costs and quality of care.

References

Adams, Katie. 2024. "AHA Urges Labor Department to Investigate MultiPlan's 'Unconscionable Practices.'" *Med City News.* April. https://medcitynews.com/2024/04/aha-insurance-healthcare-multiplan/ (accessed July 2, 2024).

AHA (American Hospital Association). 2020. "Fact Sheet: Uncompensated Hospital Care Cost." https://www.aha.org/fact-sheets/2020-01-06-fact-sheet-uncompensated-hospital-care-cost (accessed May 12, 2024)

Ak, Abhishek and Ankur Verma. 2024. “Economic Oasis: How Revenue Cycle Management is Emerging as an Investment Beacon.” Blog. Everest Group. April 10. https://www.everestgrp.com/business-process-services/economic-oasis-revenue-cycle-management-thriving-through-turbulent-times-blog.html (accessed November 5, 2024).

Alder, Steve. 2024b. “Healthcare Data Breach Statistics.” *The HIPAA Journal*. June 20. https://www.hipaajournal.com/healthcare-data-breach-statistics/ (accessed June 22, 2024).

AMA. 2024. “Change Healthcare Cyberattack Impact.” https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf (accessed May 22, 2024).

Appelbaum, Eileen, and Rosemary Batt. 2020. “Private Equity Buyouts in Healthcare: Who Wins, Who Loses?” Working Paper No. 118 Institute for New Economic Thinking. March 15. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3593887; Private Equity Buyouts in Healthcare: Who Wins, Who Loses? – Center for Economic and Policy Research (cepr.net)

Bannow, Tara. 2019. “Few Hospitals Aggressively Sue Patients to Pay Bills, and Some Don’t Bother at All,” *Modern Healthcare*, October 5. https://www.modernhealthcare.com/revenue-cycle/few-hospitals-aggressively-sue-patients-pay-bills-and-some-dont-bother-all?utm_source=modern-healthcare-am-wednesday&utm_medium=email&utm_campaign=20191008&utm_content=article2-headline (accessed January 23, 2020).

Barkholz, Dave. 2017. “After Years of Turmoil, Accretive Health Ditches Name.” *Crain’s Chicago Business*. January 5 https://www.chicagobusiness.com/article/20170105/NEWS03/170109914/after-years-of-turmoil-accretive-health-ditches-name (accessed July 20, 2024)

Bell, Allison. 2024. “MultiPlan Faces Barrage of Price-Fixing Suits in New York.” *Benefits Pro*, June. https://www.benefitspro.com/2024/06/10/multiplan-faces-barrage-of-price-fixing-suits-in-new-york/.

Businesswire. 2023. “Change Healthcare Research: AI to Become Widespread in Hospital Revenue Cycle by 2023.” https://www.businesswire.com/news/home/20210119005151/en/Change-Healthcare-Research-AI-to-Become-Widespread-in-Hospital-Revenue-Cycle-by-2023 (accessed June 6, 2024).

Cass, Andrew. 2024. “UnitedHealth Group in the Headline: 12 Updates.” *Becker’s Payer’s Issues*. July 22. https://www.beckerspayer.com/payer/unitedhealth-group-in-the-headline-12-updates.html?utm_campaign=payer&utm_source=website&utm_content=latestarticles (accessed July 23, 2024)

CBS News. 2012. “MNs AG Releases Scathing Report on Accretive Health Inc.” *CBS News.* April 24. https://www.cbsnews.com/minnesota/news/mns-ag-releases-scathing-report-on-accretive-health-inc/ (accessed July 20, 2024)

CFPB 2025. CFPB Finalizes Rule to Remove Medical Bills from Credit Reports. Consumer Financial Protection Bureau. January 7. https://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-rule-to-remove-medical-bills-from-credit-reports/ (accessed January 9, 2025).

CMA (Center for Medicare Advocacy). 2022. “The Role of AI-Powered Decision-Making Technology in Medicare Coverage Determinations.” *Medicare Advocacy*. January. https://medicareadvocacy.org/wp-content/uploads/2022/01/AI-Tools-In-Medicare.pdf (accessed August 1, 2024)

CMS. 2024. “Hospital Price Transparency.” Centers for Medicare and Medicaid Services. September 9. https://www.cms.gov/priorities/key-initiatives/hospital-price-transparency/hospitals (accessed January 7, 2025).

Cohen, Robin, Brian W. Ward, and Jeannine S. Schiller. 2011. “Health Insurance Coverage: Early Release of Estimates from the National Health Interview Survey, 2010.” Centers for Disease Control. https://www.cdc.gov/nchs/data/nhis/earlyrelease/insur201106.htm (accessed July 26, 2024)

CommonWell Health Alliance. 2014. “Overview Fact Sheet.” September 30. http://www.commonwellalliance.org/wp-content/uploads/2014/10/CommonWell-Overview-FactSheet-30Sept2014.pdf (accessed July 31, 2024).

Couey, Collin. 2024. “More Than One in Four Ransomware Attacks on Healthcare Organizations Affect Patient Care.” *Software Advice*. May 21. https://www.softwareadvice.com/resources/healthcare-cybersecurity-threat/ (accessed July 22, 2024)

Crowe RCA Benchmarking Analysis. 2018. Considering Revenue Cycle Outsourcing? Look (Here) Before You Leap. August. https://www.crowe.com/-/media/Crowe/LLP/folio-pdf-hidden/Benchmarking-Report-Q2-HC-19006-012A.ashx?la=en-US&hash=01900EF19DAD890CF6B3A0543EDC71FCA038EA60 (accessed June 10, 2024)

Dayen, David. 2023. “Patient Zero.” *The American Prospect*, August 1. https://prospect.org/health/2023-08-01-patient-zero-tom-scully/ (accessed September 22, 2023)

Delancey Street Partners, LLC. 2022. “Revenue Cycle Management – Sector Review. 2022. https://www.delanceystreetpartners.com/wp-content/uploads/2022/09/RCM-Services-Sector-Review.pdf (accessed May 14, 2024).

Energy and Commerce Committee, U.S. Congress. 2024. “What We Learned: Change Healthcare Cyber Attack.” May 3. https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack (accessed July 23, 2024)

Fenne, Michael. 2024. “Private Equity’s Revenue Cycle: Creating and Collecting U.S. Medical Debt.” Private Equity Stakeholder Project. September. https://pestakeholder.org/reports/private-equitys-revenue-cycle-creating-and-collecting-u-s-medical-debt/ (accessed December 2, 2024).

FTC (Federal Trade Commission). 2024a. “FTC Finalizes Changes to the Health Breach Notification Rule.” April 26. https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule (accessed May 16, 2024)

FTC. 2024b. “BetterHelp Refunds.” June. https://www.ftc.gov/enforcement/refunds/betterhelp-refunds (accessed July 22, 2024).

Grand View Research. 2023. “U.S. Revenue Cycle Management Market Size, 2030.” Grand View Research. https://www.grandviewresearch.com/industry-analysis/us-revenue-cycle-management-rcm-market?gad_source=1# (accessed January 8, 2025).

Hagland, Mark. 2021. “Is AI in Revenue Cycle’s Future? Experts Say the Answer is a Clear ‘Yes, But’”. *Healthcare Innovation*. Sept. 20. https://www.hcinnovationgroup.com/finance-revenue-cycle/revenue-cycle-management/article/21236362/is-ai-in-revenue-cycles-future-experts-say-the-answer-is-a-clear-yes-but (accessed June 22, 2024)

Halleman, Sydney. 2023a. “Johns Hopkins hit with class action suit following data breach. *Healthcare Dive.* July 12. https://www.healthcaredive.com/news/johns-hopkins-hit-with-class-action-suit-data-breach/686650/ (accessed May 26, 2024)

Halleman, Sydney. 2023b. “Thoma Bravo Closes $1.8B Deal to Take Nextgen Healthcare Private.” *Healthcare Dive*. Nov. 10. https://www.healthcaredive.com/news/thoma-bravo-acquires-nextgen-healthcare/692792/

Hamby, Chris. 2024a. “Insurers Reap Hidden Fees by Slashing Payments. You May Get the Bill.” *The New York Times.* April. https://www.nytimes.com/2024/04/07/us/health-insurance-medical-bills.html (accessed May 14, 2024)

Hamby, Chris. 2024b. “Senators See Possible Conflict of Interest in Company’s Health Care Pricing Tools.” *The New York Times*. May 28. https://www.nytimes.com/2024/05/28/us/senate-multiplan-health-care-pricing.html (accessed May 30, 2024)

Hansei. 2024. “A Beginner’s Guide to End-to-End Revenue Cycle Management.” https://hanseisolutions.com/a-beginners-guide-to-end-to-end-revenue-cycle-management/ (accessed June 14, 2024).

Herman, Bob. 2023. Medicare Advantage Plans Will Have to Stop Denying Required Care, Federal Officials Say. *STAT News*. April 5. https://www.statnews.com/2023/04/05/medicare-advantage-denying-care/ (May 4, 2023)

Herman, Bob. 2024. "Private Equity Firms to Acquire Health Care Billing And Payments Firm R1 In $8.9 Billion Deal. *STAT News*. Aug. 1. https://www.statnews.com/2024/08/01/r1-rcm-deal-towerbrook-cdr/ (accessed August 4, 2024)

Herman, Bob, and Casey Ross. 2023a. "Senators Probing Largest Medicare Advantage Plans Over How Algorithms Factor in Care Denials." *STAT News.* May 17. https://www.statnews.com/2023/05/17/senate-investigation-medicare-advantage-algorithms-denials/ (access May 20, 2023)

Herman, Bob, and Casey Ross. 2023b. "UnitedHealth Faces Class Action Lawsuit Over Algorithmic Care Denials in Medicare Advantage Plans." *STAT News.* Nov 14. https://www.statnews.com/2023/11/14/unitedhealth-class-action-lawsuit-algorithm-medicare-advantage/ (accessed Jan. 5, 2024)

Herman, Bob, and Casey Ross. 2023c. "UnitedHealth Used Secret Rules to Restrict Rehab Care for Seriously Ill Medicare Advantage Patients." *STAT News.* Dec. 28. https://www.statnews.com/2023/12/28/medicare-advantage-united-health-navihealth-rehab-care-restrictions/ (accessed Jan. 5, 2024)

Herman, Bob, and Casey Ross. 2024. "UnitedHealth Argues Algorithm Lawsuit Should Be Dismissed Because Patients Didn't Spend Years Appealing Denials." *STAT News.* May 22. https://www.statnews.com/2024/05/22/unitedhealth-class-action-lawsuit-algorithm-motion-to-dismiss/ (accessed May 28, 2024)

Hoffman, Liz. 2016. "How four private equity firms cleaned up on MultiPlan. *Financial* News *London*. May 9. https://www.fnlondon.com/articles/how-private-equity-firms-cleaned-up-on-multiplan-20160509 (accessed June 6, 2024)

Humbert, Mathias, et al. 2015. "De-anonymizing Genomic Databases Using Phenotypic Traits." *Proceedings on Privacy Enhancing Technologies.* 2:99-114. https://hal.science/hal-01151960/

IBM. 2023. "Cost of a Data Breach Report 2023." *IBM Security*. https://www.ibm.com/downloads/cas/E3G5JMBP (accessed July 22, 2024)

Kacik, Alex. 2024. "Higher Fines Compel Most Hospitals to Disclose Prices." *Modern Healthcare*. April 04. https://www.modernhealthcare.com/providers/price-transparency-fines-cms (accessed June 23, 2024).

Kadepalli, Srinivas. 2019. “Should You Outsource Your Revenue Cycle Management?” *Invensis.* October 18. https://www.invensis.net/blog/healthcare/rcm-outsourcing/ (accessed July 1, 2024).

Kasprak, John. 2008. “Federal Appellate Court Decision — New Hampshire Prescription Drug Information Law.” OLR Research Report. December 4. https://www.cga.ct.gov/2008/rpt/2008-r-0680.htm (accessed July 1, 2024)

Kieffer, J. 2023. “The Definitive Guide to Revenue Cycle Management.” May 30. *Fierce Healthcare.* Nov 22. https://www.fiercehealthcare.com/tech/two-private-equity-firms-near-17b-deal-to-acquire-athenahealth-wsj-report (accessed July 28, 2024)

Kutscher, Beth. 2015. Hospitals turn to friendlier tools to collect unpaid bills. Modern Healthcare. May 16. https://www.modernhealthcare.com/article/20150516/MAGAZINE/305169974/hospitals-turn-to-friendlier-tools-to-collect-unpaid-bills (accessed June 20, 2020).

Jacqueline, LaPointe. 2018. “80% of Hospitals Vetting Full Revenue Cycle Management Outsourcing,” *Revcycle Intelligence*. May 14. https://revcycleintelligence.com/news/80-of-hospitals-vetting-full-revenue-cycle-management-outsourcing (accessed January 23 2020).

LaPointe, Jacqueline. 2023. “Generative AI’s Potential Shines on Revenue Cycle Management.” *Revcycle Intelligence.* October 19 https://revcycleintelligence.com/features/generative-ais-potential-shines-on-revenue-cycle-management (accessed November 20, 2024).

Liss, Samantha. 2022. “Judge Denies DOJ’s Move to Block $13B UnitedHealth, Change Deal.” *Healthcare Dive.* Sept. 20. https://www.healthcaredive.com/news/judge-denies-dojs-move-block-unitedhealth-change-acquisition/632226/ (accessed March 15, 2024)

Loyale Healthcare. 2019. “Private Equity Investments and the Drive for Innovation in Healthcare.” *Business Insider.* September 5. https://markets.businessinsider.com/news/stocks/private-equity-investments-and-the-drive-for-innovation-in-healthcare-industry-analysis-by-loyale-healthcare-1028500970 (access May 15, 2024)

Luthra, Shefali. 2018. “Bank Loans Signed in the Hospital Leave Patients Vulnerable,” *Los Angeles Times.* February 21. https://www.latimes.com/business/la-fi-hospital-loans-20180221-story.html (accessed January 10, 2020).

Microsourcing. 2024. “The Future of Healthcare Delivery in the U.S.” https://www.microsourcing.com/future-of-healthcare-delivery-in-the-us/?utm_term=&utm_campaign=MicroSourcing%20-%20PMAX%20-%20AU%20-%20SP%20(Max%20Conv)&utm_source=adwords&utm_medium=ppc&hsa_acc=8750364042

&hsa_cam=21137899421&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1

Miliard, Mike. 2015 “Emdeon to Acquire Altegra Health.” *Healthcare IT News*. July 08. https://www.healthcareitnews.com/news/emdeon-acquire-altegra-health (accessed July 23, 2024)

Monegain, Bernie. 2011. “Emdeon Goes Private in $3B Deal. *Healthcare IT News*. August 04 https://www.healthcareitnews.com/news/emdeon-goes-private-3b-deal (accessed July 23, 2024)

Multiplan. 2024. “Form 10-K MultiPlan Corporation.” February 29. https://investors.multiplan.us/financials/sec-filings/sec-filings-details/default.aspx?FilingId=17322718

Muoio, Dave. 2024a. “Community Health Systems Adds Another Antitrust Lawsuit to MultiPlan’s Collection.” *Fierce Healthcare*, May 9. https://www.fiercehealthcare.com/payers/community-health-systems-adds-another-antitrust-lawsuit-multiplans-collection

Muoio, Dave. 2024b. “Ascension: Cyberattacker Stole Files Likely Containing Protected Health, Identity Data.” *Fierce Healthcare*. Jun 12. https://www.fiercehealthcare.com/providers/systems-clinical-operations-interrupted-ascension-amid-apparent-cybersecurity-event (accessed June 24, 2024)

NAHDO (National Association of Health Data Organizations). 2024. “Data System Tech Resources.” NAHDO. https://www.nahdo.org/data_resources

Obermeyer, Ziad, Rebecca Nissan, Michael Stern, Stephanie Eaneff, Emily Joy Bembeneck, Sendhil Mullainathan. 2021. *Algorithmic Bias Playbook*. Chicago Booth Center for Applied Artificial Intelligence. June. https://www.chicagobooth.edu/-/media/project/chicago-booth/centers/caai/docs/algorithmic-bias-playbook-june-2021.pdf (accessed July 23, 2024)

OCR (Office of Civil Rights, HHS). 2024. “Cases Currently Under Investigation.” https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=E5B93B2D9E7FC47CF1CBC28DDBF94446 (accessed July 22, 2024)

OCR/HHS. 2024. (Office for Civil Rights, Department of Health and Human Services). “Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information.” https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=A4255C9C25D0C00E9E2AD4F7A51FA705 (accessed January 1, 2025)

Olsen, Emily. 2023. “HCA Faces Class Action Lawsuit After Data Breach.” *Healthcare Dive*. July 17. https://www.healthcaredive.com/news/HCA-Healthcare-faces-class-action-lawsuit-after-data-breach/687960/ (accessed May 28, 2024)

Olsen, Emily. 2024. “ONC’s Micky Tripathi on Laying the Digital Floor for Healthcare AI.” *Healthcare Dive.* June 20. https://www.healthcaredive.com/trendline/electronic-health-records/263/?utm_source=HD&utm_medium=Library&utm_campaign=Optimal&utm_term=Healthcare%20Dive%20Weekender (last accessed January 6, 2025)

Patient Privacy Rights. N.D. “Patient Privacy Rights Board and Staff.” https://patientprivacyrights.org/board-and-staff-2/ (accessed June 20, 2024)

Paavola, Alia. 2021. “Hospitals Ask Feds to Investigate UnitedHealth’s $13B Acquisition of Change Healthcare.” *Beckers Health IT*. March 19. https://www.beckershospitalreview.com/healthcare-information-technology/hospitals-ask-feds-to-investigate-unitedhealth-s-13b-acquisition-of-change-healthcare.html?utm_medium=email&utm_content=newsletter (accessed June 18, 2024)

PESP (Private Equity Stakeholder Project). 2021. “How Private Equity Profits from Aggressive Medical Debt Collection”. August 24. https://pestakeholder.org/news/how-private-equity-profits-from-aggressive-medical-debt-collection/

PitchBook. 2024a. “PitchBook_NaviHealth_2024_08_01_18_05_23.” PitchBook Data, Inc.

PitchBook. 2024b. “PitchBook_Multiplan_2024_07_31_20_48_15.” PitchBook Data, Inc.

PitchBook. 2024c. “PitchBook Change Healthcare 2024_07_31_24_12_06.” PitchBook Data, Inc.

PitchBook Conifer. 2025. “PitchBook_Conifer_Health_Solutions_2025_01_08_15_16_17.” PitchBook Data, Inc.

PitchBook Parallon. 2025. “PitchBook_Parallon_2025_01_08_15_15_46.” PitchBook Data, Inc.

Rakshit, Shameek, Matthew Rae, Gary Claxton, Krutika Amin, and Cynthia Cox. 2024. The Burden of Medical Debt In The United States. Kaufman Family Foundation. February 12. https://www.healthsystemtracker.org/brief/the-burden-of-medical-debt-in-the-united-states/#Share%20of%20adults%20who%20have%20medical%20debt,%20by%20demographics,%202021 (accessed June 20, 2024)

Reuters. 2012. “S&P Rates Emdeon Inc Snr Secured Credit Facilities.” April 23. https://www.reuters.com/article/business/media-telecom/sp-rates-emdeon-inc-snr-secured-credit-facilities-idUSWNA5571/ (accessed March 12, 2024).

Riggi, John. 2024. “A High-Level Guide for Hospital and Health System Senior Leaders.” American Hospital Association. Https://Www.Aha.Org/Center/Cybersecurity-And-Risk-Advisory-Services/Importance-Cybersecurity-Protecting-Patient-Safety (accessed July 23, 2024)

Rosato, Donna. 2018. “Should You Ever Prepay a Hospital Bill?” *Consumer Reports.* April 12. https://www.consumerreports.org/healthcare-costs/prepay-hospital-bill/ (January 10, 2020).

Ross, Casey. 2021a. ‘Nobody Is Catching It’: Algorithms Used in Health Care Nationwide Are Rife with Bias.” *STAT News*. June 21. https://www.statnews.com/2021/06/21/algorithm-bias-playbook-hospitals/ (accessed July 12, 2023)

Ross, Casey. 2021b. “Epic’s AI Algorithms, Shielded from Scrutiny By A Corporate Firewall, Are Delivering Inaccurate Information on Seriously Ill Patients.” *STAT News*. July 26. https://www.statnews.com/2021/07/26/epic-hospital-algorithms-sepsis-investigation/ (accessed July 12, 2023)

Ross, Casey. 2022a. “Once Billed as a Revolution in Medicine, IBM’s Watson Health Is Sold Off in Parts.” *STAT News*. Jan 21. https://www.statnews.com/2022/01/21/ibm-watson-health-sale-equity/ (accessed July 12, 2023)

Ross, Casey. 2022b. “AI Gone Astray: How Subtle Shifts in Patient Data Send Popular Algorithms Reeling, Undermining Patient Safety.” *STAT News*. Feb. 28. https://www.statnews.com/2022/02/28/sepsis-hospital-algorithms-data-shift/ (accessed July 12, 2023)

Ross, Casey and Bob Herman. 2023a. “Denied by AI: How Medicare Advantage Plans Use Algorithms to Cut Off Care for Seniors in Need. *STAT News*. March 13. https://www.statnews.com/2023/03/13/medicare-advantage-plans-denial-artificial-intelligence/ (accessed July 12, 2023)

Ross, Casey and Bob Herman. 2023b. “UnitedHealth Pushed Employees to Follow an Algorithm to Cut Off Medicare Patients’ Rehab Care. *STAT News*. November 11.

https://www.statnews.com/2023/11/14/unitedhealth-algorithm-medicare-advantage-investigation/ (accessed December 2, 2023)

Rundle, James. 2024. “Hackers Broke into Change Healthcare’s Systems Days Before Cyberattack.” *Wall Street Journal*. April 22. https://www.wsj.com/articles/change-healthcare-hackers-broke-in-nine-days-before-ransomware-attack-7119fdc6 (accessed May 15, 2024)

Sage HarrisWilliams. 2024. “The Current and Future State of Revenue Cycle Management—Market and M&A Trends.” https://go.sage-growth.com/l/234212/2024-05-16/3m4f8v/234212/1715889419pKbp4zFq/Sage_Growth_Market_Report_The_Current_and_Future_State_of_Revenue_Cycl.pdf?utm_source=HarrisWilliams&utm_medium=Website&utm_content=Market-Report&utm_campaign=HW+Market+Report (accessed January 8, 2025).

Schmidt, Michelle. 2016. “The Link Between Patient Satisfaction and RCM Outsourcing,” The Midland Group. February 8. https://www.midlandgroup.com/blog/the-link-between-patient-satisfaction-and-rcm-outsourcing/ (accessed Jun 2, 2024)

Scott, Ronald. 1999. “Privacy of Pharmacy Records.” https://www.law.uh.edu/healthlaw/perspectives/HealthPolicy/990331Pharmacy.html (accessed July 20, 2024)

Singh, Karandeep. 2021. “Evaluating a Widely Implemented Proprietary Deterioration Index Model among Hospitalized Patients with COVID-19.” *Ann Am Thorac Soc*., 18(7): 1129–1137. https://www.atsjournals.org/doi/pdf/10.1513/AnnalsATS.202006-698OC

SNS Insider. 2022a. Electronic Health Records (EHR) Market Size Share Segmentation by Product (Client Server-Based HER, Web-Based HER), By Type (Acute, Ambulatory, Post-Acute), By Business Models, By End Use, By Region | Global Market Forecasts 2024-2032. May. Report Code: SNS/HC/1044. https://www.snsinsider.com/reports/electronic-health-records-ehr-market-1044 (accessed July 7, 2024).

SNS Insider. 2022b. “Healthcare IT Outsourcing Market Size, Share & Segment by Application (Provider Outsourcing Market, Payer Outsourcing Market, Life Science Outsourcing Market, Operational Outsourcing Market, Infrastructure Outsourcing Market), By Industry (Healthcare System, Healthcare Insurance Industry, Pharmaceutical Industry, Clinical Research Organization, Biotechnology), by Regions and Global Forecast 2024-2031. July. Report Code: SNS/HC/2428. https://www.snsinsider.com/reports/healthcare-it-outsourcing-market-2428 (accessed July 7, 2024).

Sorrell v. IMS Health, Inc., 564 U.S. 552 (2011) https://supreme.justia.com/cases/federal/us/564/552/

Southwick, Ron. 2024 “Change Healthcare Cyberattack: VA Notifies 15 Million Veterans About Breach.” *Chief Healthcare Executive.* April 27 https://www.chiefhealthcareexecutive.com/view/change-healthcare-cyberattack-va-notifies-15-million-veterans-about-breach (accessed May 16, 2024)

Sweeney L. 2015. “Only You, Your Doctor, and Many Others May Know.” *Technology Science.* 2015092903. September 28. https://techscience.org/a/2015092903/

Tanner, Adam. 2017. *Our Bodies, Our Data: How Companies Make Billions Selling Our Medical Records*. Cambridge: Beacon Press.

Tornone, Kate. 2020. “NaviHealth Pays Nearly $4.7M to Settle Misclassification Suit.” *Healthcare Dive.* May 14. https://www.hrdive.com/news/navihealth-pays-nearly-47m-to-settle-misclassification-suit/577950/ (accessed July 30, 2024).

Tozzi, John, and Zachary Tracer. 2018. “Sky-High Deductibles Broke the U.S. Health Insurance System,” *Bloomberg.* June 26. https://www.bloomberg.com/news/features/2018-06-26/sky-high-deductibles-broke-the-u-s-health-insurance-system (accessed May 20, 2024).

TSI 2025. “Healthcare.” https://gotsi.com/jmw/industries/healthcare (accessed January 9, 2025).

U.S. BLS (Bureau of Labor Statistics). 2024. “Employee Benefits: High Deductible Health Plans and Health Savings Accounts.” Washington, D.C. U.S. BLS. https://www.bls.gov/ebs/factsheets/high-deductible-health-plans-and-health-savings-accounts.htm (accessed July 26, 2024)

U.S. Census. 2023. “HIC-4_ACS. Health Insurance Coverage Status and Type of Coverage by State – All Persons 2008 to 2022.” https://www2.census.gov/programs-surveys/demo/tables/health-insurance/time-series/acs/hic04_acs.xlsx (accessed July 26, 2024)

U.S. HHS (Department of Health and Human Services). 2018. “Health Care Industry Cybersecurity Task Force.” November 27. https://www.phe.gov/Preparedness/planning/CyberTF/Pages/default.aspx (accessed May 15, 2024).

U.S. HHS. 2023a. “Hospital Cyber Resiliency Initiative Landscape Analysis.” https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf (accessed May 15, 2024).

U.S. HHS. 2023b. “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.” https://405d.hhs.gov/Documents/HICP-Main-508.pdf (accessed May 15, 2024).

U.S. HHS 405(d). N. D. “Aligning Health Care Industry Security Approaches. https://405d.hhs.gov/ (accessed May 15, 2024).

Ubhi, Raja. 2024. “10 Largest RCM Companies.” April 16. https://medium.com/@kaku1006/top-10-revenue-cycle-management-rcm-companies-in-the-usa-2d4df702d4f2 (accessed July 30, 2024)

Vogel, Susanna. 2024. “Ascension Hit with Lawsuits Days After Ransomware Attack. *Healthcare Dive.* May 16. https://www.healthcaredive.com/news/ascension-lawsuits-ransomware-attack-cybersecurity/716248/ (accessed May 28, 2024)

Zeitner, Daniel. 2019. “Outsourced Revenue Cycle Services 2019: Are Outsourced Revenue Cycle Services Worth the Investment?” KLAS Research. June 25. https://klasresearch.com/report/outsourced-revenue-cycle-services-2019-are-outsourced-revenue-cycle-services-worth-the-investment/1467 (accessed July 3, 2024).

Endnotes

1. For a detailed account of the evolution of private equity in RCMs and medical debt collection, see Eileen Appelbaum and Rosemary Batt. 2020. Private Equity Buyouts in Healthcare: Who Wins, Who Loses?" Working Paper No. 118 Institute for New Economic Thinking, pp 76-93. March 15. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3593887
2. A full analysis of the OCR/HHS trend data, along with healthcare organization, year, type, and numbers affected for each attack are found in Alder (2024b).