CHAPTER 6

WHY HEALTHCARE COMPLIANCE ANALYTICS? WHY NOW?

Robert Lord

§ 6.01 OVERVIEW OF HEALTH CARE COMPLIANCE ANALYTICS

At its essence, healthcare compliance analytics (HCA) is a methodology for streamlining compliance workflows, helping teams find risks that previously were hidden, and focusing the legal and compliance teams' energy on real threats, rather than false positives. Through adopting an HCA approach, health systems actively reduce risks, rather than just manage them.

You might be reading this chapter to refine your current HCA practice. You might be reading this chapter in order to learn more about the HCA trend you are hearing about from your colleagues. You might be wondering, "what the heck is HCA?" This chapter is designed for all three types of readers noted above, and we hope everyone from beginners to advanced practitioners will find something useful herein. Because HCA is a relatively recent trend in the industry, a brief look at the slate of privacy, security, compliance, and legal challenges that it serves to address will be helpful. Those challenges are best illustrated with three stark dollar figures.

1. $6.2 billion.

That is the annual cost of data breaches to the health care industry.[1] Whether external hackers or, more likely, insider threats, the damage that is done every year to health systems due to malicious or naive actors compromising hospital data and electronic systems is immense. The sheer volume of attacks and huge attack surface makes complete defense, as is always the case with cybersecurity, a near-impossibility.

2. $39 billion.

That is the annual cost of complying with health care's onerous slate of regulations, ranging from the conditions of participation to Health Insurance Portability and Accountability Act (HIPAA).[2] The vast majority of this cost comes from the staff required to review reports regularly, check off proverbial boxes, and ensure that health systems are up-to-date with the latest in regulatory arcana.

3. $272 billion.

That is the amount of fraud, waste, and abuse diverted from Medicare and Medicaid used not for legitimate patient care, but rather inappropriate procedures, fraudulent transactions, or simply inefficiencies in health care processes

[1] https://www.beckershospitalreview.com/healthcare-information-technology/healthcare-breaches-cost-6-2b-annually.html.

[2] https://www.aha.org/guidesreports/2017-11-03-regulatory-overload-report.

that have gone unaddressed.[3] With so much complexity and dependency in our systems, it is extremely difficult for health systems and regulators to discern what constitutes appropriate versus inappropriate care.

While these more-than-$300 billion-total challenges appear highly disparate, they are, in fact, all connected to the very same issue: we have too many activities being performed in too many systems to have any hope of humans being able to collate, track, and judge each of them. There is simply too much going on in health care to have any reasonable hope of proactively isolating signal from noise. Whether patient care in the electronic health record (EHR), ordering from procurement, billing system automation, or the hundreds of other highly regulated activities performed every day in a health system, there is simply too much for any one legal or compliance team to handle.

This problem of volume, velocity, and variety of data is, no doubt, familiar to the compliance and legal professionals. Often times, issues only get to your desk when a complaint comes in, though examination of the facts reveals that this could have been predicted beforehand had someone been looking closely.

HCA offers a new approach. In a model driven by HCA, all the data you need to verify if you are in compliance and actively managing your risks is centralized for your easy review. You are assured in the real-time auditing of every action taken in your health system, and you know that systems are in place to prove the appropriateness or inappropriateness of these actions using all of the data at hand that would normally have been used in a manual retroactive investigation. Education is delivered in an automated fashion, as needed. When something comes to your attention, you have high confidence that the case is a real violation rather than a false positive.

How is this possible, you might ask? To understand what this new paradigm looks like, let us examine how we are currently tackling these problems.

§ 6.02 THE STATUS QUO

In a modern health care system, nearly every action taken is documented electronically in some form or another. Every swipe of a card reader into a secured ward, every drug pulled out from an ADC, every view of a medical record, and every review done on a note for billing verification. We even document our documentation, reporting out on our levels of compliance and reporting, to ensure concordance with an ever-increasing landscape of regulations.

We are accountable to a wide array of institutions, whether Centers for Medicare and Medicaid Services (CMS), the Joint Commission, state licensing boards, HHS-OCR, or hundreds of other entities. But this accountability is largely mediated through a retroactive approach, where we regularly perform "spot

[3] https://www.economist.com/united-states/2014/05/31/the-272-billion-swindle.

checks" and report out on metrics, looking at perhaps 1 percent or less of activities to demonstrate that all of the rules are being followed. The other 99 percent of activities we hold in "cold storage," available for retroactive inspection if necessary, but mostly never seeing the light of day.

However, while we document everything and store it away should we ever need to prove it was appropriate, we in no way proactively demonstrate that each of these actions taken were actually appropriate. All too often, when something goes horribly wrong, we can look back and tell ourselves . . .

> ". . . wow, nursing prescribing practices have been all wrong for years,"
>
> or
>
> ". . . I can't believe that we've been inappropriately coding this procedure the wrong way for a decade," or
>
> ". . . it seems unconscionable that this many celebrities and department heads are regularly looked up in the EHR for staff entertainment and curiosity."

We can see what went wrong, we can prove that we had the data to know it the whole time, but because we cannot be everywhere at the same time every second of the day, we accept that there is often nothing we could have done. So we, as an industry, have come to a compromise: review a limited subset of information, based on some shared principles and knowledge of risks, in order to at least "check the box" of ensuring compliance, if not actually actively managing our complete portfolio of risks.

Bogged down by the impossibility of reviewing every clinical interaction, every touch to data, every billing event, and every login to every system at our hospitals, we do our best to stem the tide of risks. Indeed, this has truly been the best possible option for many years, as our ability to collect data has grown exponentially, but our ability to review it has merely grown in fits and starts, largely predicated by how many humans we assign to review that data, and how many reports we run and hold ourselves accountable to.

§ 6.03 THE CONSEQUENCES OF A REPORT-DRIVEN WORLD

There is a saying among HCA specialists—"Where there are highlighters, there's opportunity."

This might seem a strange axiom, but it comes from the insight that all too many processes in compliance rely on vast amounts of information being manually reviewed by a human being who leverages their clinical and/or administrative expertise to spot anomalies—literally or virtually "highlighting" areas that might need further investigation. Usually, what they are reviewing are reports—tables, charts, graphs, printouts, logs, and more, the raw data that makes up the grist of a compliance workload.

The toll that this takes on a health system's legal and compliance teams is considerable, both in the effort expended, as well as what is missed. Running reports and manually reviewing them is both inefficient and ineffective—it is pouring a huge amount of resources into an ineffective paradigm.

As far as the effort expended, a recent American Hospital Association research endeavor notes that hospitals spend roughly $7 million per hospital facility per year merely to remain compliant, with roughly 60 full-time equivalents (FTEs) per hospital required to assess and address the risks present in their institutions.[4] Despite this, outcomes on key areas of compliance, the theoretical reason for these costs, remain dismal.

Data breaches abound in the U.S. health care system, with approximately $6.5 billion in annual damage attributable to such breaches.[5] Human beings are often forced to manually review various types of event and access logs, which are generated by the millions each day for a given health system. As a result, only a fraction of a percent of events are reviewed, with enormous amounts of effort expended to yield very little in terms of true threats. This type of approach does little to reduce institutional risk associated with data breaches.

Another example of the dangers of a report-driven world comes from our nation's opioid epidemic and health system obligations to prevent diversion of controlled substances. Huge quantities of opioids are diverted annually, with over 47 million doses of controlled substances diverted each year from health care facilities.[6] Currently, pharmacy, nursing, risk, and compliance teams are using reports to detect individuals who might be pulling high volumes of opioids, or focusing on particularly dangerous substances like fentanyl, but are still stymied by the huge volume of drug transactions that occur every day. Universal vigilance and review is simply impossible in a report-driven world. These are just two examples of the types of threats that hospitals must mitigate and the types of regulatory and compliance pressure they face.

§ 6.04 TIME FOR A NEW APPROACH

New technologies and approaches are, thankfully, emerging to address many of the challenges described above. Rather than theory, we will examine some new approaches, recently made possible by technological innovation, that are driving a new paradigm in health care law and compliance, ones that leverage artificial intelligence (AI) and "big data" solutions to substantially and demonstrably reduce risk, rather than just meet bare minimum requirements. We will not

[4] https://www.aha.org/guidesreports/2017-11-03-regulatory-overload-report.

[5] https://www.beckershospitalreview.com/healthcare-information-technology/healthcare-breaches-cost-6-2b-annually.html.

[6] 2019 Protenus Diversion Digest, Protenus, April 2019.

discuss specific technologies or platforms, as our goal is not commercial, but rather provide some examples and considerations below in purchasing such technologies. The goal is to paint a picture of two contrasting approaches.

We contrast below the historical "report driven" model with the HCA model that is now emerging, and how it changes the risk profile for a health care institution. Four key areas are being transformed by HCA technology: systems of record, automated education, complete audit verification, and accurate alerting.

[A] A Single "System of Record" Aids Investigation

A recurring issue faced by legal and compliance teams across a wide array of challenges is having all the information needed to complete an investigation available upfront. Not only does a "big data" system of record contain all of the information generated by legal and compliance teams (e.g., investigation notes, confirmation of education delivered, audit results), but also all of the data needed to complete these investigations (e.g., raw audit logs, clearly structured clinical histories, detailed billing records).

In the historical report-driven model, no single system of record housed everything—even a top-of-the line GRC solution would contain notes and record samples, rather than the complete, a priori information needed in the first place for an investigation. This model had a variety of implications, the most significant of which was considerable friction in requesting records, interpreting and explaining them, writing them up, and storing them. Often times, logs would need to be requested from IT, financial information from billing, clinical notes from charge nurses, and many other departments. This complexity led to inefficient and slow workflows for anything from a quality investigation to a billing anomaly.

In an HCA model, all relevant data sources are brought together into a single workflow, so data gathering, investigation, documentation, and resolution, along with long-term tracking, are all in a single location. What once might have been a series of data requests, a manual write-up, and an import to a governance, risk and compliance (GRC) is now a single, unified workflow that contains everything necessary in one place.

The key business driver for such an innovation is, of course, the ability to save time and reduce complexity, as well as have confidence that data are not slipping through the cracks.

[B] Automated Education Reduces Repeat Offenders

It is an all-too-clear reality that when it comes to compliance violations, repeat offenders are the norm, rather than the exception. Studies suggest that 70

percent of individuals who violate patient privacy, for instance, will do so again in the future.[7]

In a report-driven model, when a violation or risk is detected, it usually comes significantly after the fact. For instance, if you are running a monthly audit on every individual who looks themselves up in the EHR, a policy violation for your institution, you then must act on the results of such a report, sending out individual or templated emails to each detected violator. You must then record the action with a system that allows for more stringent action if individuals repeat the action, and document your notice and education for future records.

However, with HCA, certain classes of compliance violation can immediately and automatically trigger tailored education, with a targeted email sent to a first-time offender, educating them about the relevant policy. While this does not work for serious infractions that may need immediate follow-up, it allows for the triage of everyday events that would otherwise consume compliance and legal time, and not be an efficient use of such expert resources.

The aforementioned study demonstrated that those 70 percent repeat offender rates can be reduced to 2 percent for certain classes of low-level privacy violations through HCA's deployment of automated education.[8]

[C] Complete Audit Verification Provides a More Complete Defense

Another example of the power of compliance analytics comes not necessarily in what is found, but what can be proved you examined without finding anything after-the-fact. As an example, one might take a common scenario, a retroactive audit of one's billing practices, perhaps brought on by reporting of anomalies or a complaint from a patient to a government agency.

In an older, report-driven paradigm, what you would have available are records that you performed an annual audit, and hired an audit firm to review perhaps a thousand charts at random out of several hundred thousand (in a very rigorous model). You can show that you "checked the box" by doing an audit, but you certainly cannot demonstrate that every chart was reviewed and compliance was assured by comparing the patient's clinical course to the billing that was ultimately done. You are compliant, but risks still abound in the 99 percent of records that you did not check creating significant institutional liability. Should you have to go to court or defend against a regulatory action, you have no documentation or proof of auditing 99 percent of your records, and merely rely on the defense of "we did our best."

---

[7] Artificial Intelligence Helps Put Privacy on Autopilot, Johns Hopkins Health System, HIMSS 2019 Presentation.

[8] Artificial Intelligence Helps Put Privacy on Autopilot, Johns Hopkins Health System, HIMSS 2019 Presentation.

In an HCA model, your workflow is dramatically different. By examining every single billing event and comparing it to all of the associated documentation using "big data" tools, you have the capability to provide evidence of review of 100 percent of billing actions, and an AI-driven explanation of why each one was appropriate or inappropriate. While no system is perfect, you are actively rooting out risks, and clearly demonstrating that you are able to articulate why each billing activity made sense given the clinical course of a patient. Importantly, these comprehensive audit reports provide natural-language explanations of why an event was deemed appropriate or not, leveraging AI to reason out and document each event.

Only with HCA is a compliance team capable of having real confidence that they have looked beneath the proverbial surface, shining light on all of the dark corners of the organization.

[D] Accurate Detection with Clinical Context

All of the above-noted advances are not too helpful without a system that is accurately detecting potential compliance violations, as they would simply create too much noise. Advances in behavioral analytics that leverage clinical and administrative knowledge are dramatically changing the accuracy of our detection systems.

In a report-based model, regular reports might be run to detect a wide array of dangerous activities. Perhaps you look at your highest-earning physicians and their Relative Value Units (RVUs) each month to check for impossible billing patterns. Perhaps reports are regularly run to see which third-party vendors are logging into our networks off-hours. Perhaps you are looking at which nurses have the highest levels of opioid administration. Some of these procedures might be done by pharmacy or security, but the reality is that they will ultimately get to your desk if something is awry. However, all-too-often there is a perfectly reasonable explanation that could have been discerned with a deeper-dive in the data by a trained investigator. Thus, a "false positive" is created that wastes quite a bit of time. Sadly, from our experience, for many classes of compliance alert false positive rates can exceed 95 percent, meaning that most of the time spent on resolving these threats goes to waste.

In an HCA-based model, driven off of the aforementioned comprehensive review process done by AI systems, cases are only brought to your attention when no plausible reason can be found for a suspicious activity. For instance, should a nurse have a high number of opioid pulls, her past history would be automatically examined, cross-referenced with the pain control needs of her patients, she would be automatically compared to peers in similarly situated roles, and every transaction of controlled substances would be reviewed to get a sense of any potential

loss over time. Only when these angles, and hundreds more, were examined and found suspicious, would such a case be brought to the attention of a pharmacy, risk, and/or compliance team. With this type of model, a less than 5 percent false positives rate is possible, leading to robust compliance without wasted attorney and compliance officer time.

§ 6.05 HALLMARKS OF HEALTH CARE COMPLIANCE ANALYTICS

While different technologies abound for achieving the above-noted goals, some key hallmarks of an HCA system (rather than a report-driven) system are helpful to understand. We classify the key components of an HCA program in five areas (see Figure 6-1): (1) integrate, (2) audit, (3) focus, (4) resolve, and (5) learn. Some of these components have sub-components, as we note below.

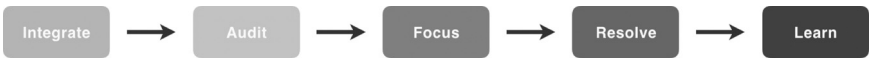

Figure 6-1: Five Key Health Care Analytics Components

Integrate: All the Data in Once Place

HCA-driven approaches have a centralized "System of Record" that houses all relevant information needed to conduct an investigation, not just store the results of an investigation. With this system of record, you should be able to examine the detailed transactions and data that led to a given conclusion or case, rather than have to request any data from other teams or sources.

Audit: Prove 100 Percent Audit and Documentation

Any HCA system *must* be able to prove that it has reviewed 100 percent of actions. Explanations should be present for all of the millions or billions of events of interest, and clear reasons why they have been ruled in or out must be available should you ever want to look back and see why a decision was made.

Focus: Clinical Context-Rich

HCA is unique in its understanding of complex health care workflows, which aids in its ability to remove false positives and find subtle threats. By being able to behaviorally differentiate a cardiologist from an endocrinologist, know what procedures make sense for a patient or not, and know how EHRs are used by appropriate users versus compromised credential users, HCA-driven teams can find needles in haystacks with ease.

Resolve: Cases, Not Alerts

An HCA system is distinguished from a report-based system by accurate, natural language cases that display all relevant information and reasons for a case being presented. If you are looking at lists of activities that do not conform to a particular rule, those are reports. If you are looking at something that fully describes all the angles and tells you why this is definitively a violation, that is HCA.

Resolve: Workflow Efficiency

HCA is, at its core, all about a unified workflow for resolving cases. Rather than jumping from system to system and calling on multiple departments, HCA-driven teams are rapidly resolving cases and trivial tasks are automated to allow teams to focus on important ones.

Learn: Automate Education

HCA, in its focus on making sure legal and compliance teams are examining strategic risks, rather than every day automatable tasks, should be taking some mundane activities off of the plates of compliance teams. Low-level risks can often be addressed by targeted education and policy reminders, along with automated tracking and escalation should someone repeat the offense.

Learn: ROI Tracking

HCA is all about data, and as a result, it should be able to prove its efficacy. HCA systems should have robust capabilities to demonstrate what they have found over time, break it down by role, facility, violation type, and more, and show how culture is measurably improving over time. The heart of an HCA program is the reduction in risk that occurs over time, so without this demonstration, you are missing the final, most important piece.

§ 6.06 SELECTING AN HCA SYSTEM

We provide below a brief narrative "checklist" for components to consider and features to examine when selecting an HCA system.

Factor 1: Total Cost of Ownership

Consider the true total cost of ownership (TCO). It is important to consider the cost of the status quo, essentially the cost of inaction.

Key areas to consider when creating a TCO analysis are:

1. What level of false positives do you expect with a system that will need to be manually reviewed?
2. How much time does your current workflow consume to bring data sources together?
3. How many FTEs do you currently use to complete this function? How many consultant hours?
4. What is the risk to your institution from a financial perspective with and without a solution? (e.g., reputational, regulatory, direct cost, etc.)
5. What is the difference in cost of a single event if proactively detected versus after the fact?

Factor 2: Resources Deployed

Another key set of considerations is what you will have available in terms of budget and personnel, beyond your TCO calculation. For instance, if only a fraction of an FTE is allocated to a particular function, you want to ensure that whatever system and protocols you put in place only produces highly accurate alerts, so that they can be addressed quickly. Conversely, with a large team, you will want to ensure that you have robust collaboration and reporting tools, since that can be a challenge the larger a team gets.

Factor 3: Existing and Future Stakeholders

When purchasing a system and/or designing an HCA plan, it is important to consider all the potential stakeholders involved. Considering the roles of risk, human resources, compliance, privacy, security, technology, and clinical/pharmacy teams are all critically important. Ensure that whatever processes you are setting up have institutional buy-in ahead of time to avoid challenges down the line.

Factor 4: Centralization versus Decentralization

One question many organizations face with meeting compliance requirements is whether or not to reorganize various functions into their respective facilities versus centralized compliance across an entire health system. In the long run, the power of HCA is that it is quite possible to centralize many compliance functions into a single, core office to gain both efficiency and more rapid institutional learning. However, there are often reasons to be site-specific; if this is the case, ensure that your protocols and platforms have the ability to easily drill-down and acquire permission by facility.

Factor 5: Data Sources

It is important to consider (1) what data sources you are monitoring with HCA, as well as (2) what data sources you are using to accurately detect compliance violations. We find it helpful to map out all of the data sources that a human investigator would use in the course of resolving a potential alert or complaint. If you are going to end up requesting information from clinical systems like EHRs, billing systems, pharmaceutical logs, time and attendance systems, and more, make sure that your HCA platform is capable of ingesting all of these upfront in order to take that work off your plate and remove false positives ahead of time. Dig in with any potential system to what data sources are included and how they are used.

Factor 6: Accuracy

Related to the idea of data sources is the question of accuracy. Leveraging rich clinical and administrative context drives accuracy, as one can often find reasons for a seeming anomaly if one digs deeper in varied data sources. You should target 95%+ accuracy in your alerting systems, before human intervention or managed services, in order to ensure that what is being focused on is truly a valuable alert. This accuracy should also increase over time through machine learning, in order to drive positive institutional change.

Factor 7: AI Efficiency

A hallmark of an HCA system is the concept of AI efficiency, the ability to automatically review 100 percent of all events and individually risk score them, classifying them as appropriate or inappropriate. This process should be effortless, and completed by an advanced AI system. This is the *sine qua non* of an HCA system. The critical capability to take this manual work off your plate and provide natural language explanations for why an event is appropriate or inappropriate is what provides an HCA-driven institution with the peace of mind that everything is being reviewed, and that alerts are being accurately brought to your attention.

§ 6.07 KEY PERFORMANCE INDICATORS FOR A COMPLIANCE ANALYTICS PROGRAM

Whatever solution, approach, policies, and technologies you may use, a new generation of key performance indicators (KPIs) are emerging for the modern compliance department. Driving success in your organization is highly dependent on the success of the below metrics.

Breach Risk Averted

A successful HCA program helps an organization avoid risk. According to a study, the average damage done per breached healthcare record is $408.[9] Given the importance of close monitoring, an average annual calculation of risk reviewed and defended against is now more straightforward using contemporary techniques. This is an example of the type of quantification and ROI generation that, ideally, you should be able to capture with an HCA program.

Percent Records Reviewed

Many organizations presently review far below the ideal 100 percent of events in clinical and administrative systems, often due to resource, technology, or personnel limitations. Report-running and periodic reviews result in capturing perhaps 1 to 5 percent of total events, which provides a chance to catch some events, but is ultimately an unacceptable portion of events. Striving for the ability to prove that 100 percent of all events have been audited is crucial.

Policy Areas Covered (by 100 percent Review)

This metric is a measure of how many areas of your institution are protected by HCA policies and 100 percent review of events. While a somewhat subjective measure, by looking across your risk portfolio you can see how many compliance/monitoring processes are currently not reviewed by HCA, and create a roadmap for how to transition logical areas over to an HCA paradigm.

Time to Case Detection

This metric is all about institutional safety; the longer it takes to detect a policy violation, the more damage an individual can do to your health system. Right now, detection times for policy violations are abysmal, for example averaging 22 months to detect theft of controlled substances based on a recent analysis.[10] In such a long period of time, a huge number of patients and workforce members can be affected by a policy violator, continuously increasing a health system's liability.

Time to Case Resolution

The amount of time that it currently takes to resolve a case after detection is largely a measure of workforce friction in resolving a case, and mostly results from handing cases back and forth between departments. For instance, if a HIPAA

[9] Ponemon Institute—Ponemon Cost of a Breach 2019.
[10] Protenus, Inc.—Protenus Diversion Digest 2019.

privacy workflow needs privacy review, then a handoff to security, then to IT, then back to privacy, then to nursing, etc., one is likely to have a multi-week or multi-month process. However, if all of the information generated by those handoffs are presented upfront, this time to resolution may be mere minutes (or hours if an interview is required).

False Positive Rate

The false positive rate for traditional compliance monitoring programs is unacceptably high, but simultaneously a necessary evil. A false positive results from any investigation that is initiated that leads to neither an opportunity for improvement, nor a policy violation. High false positive rates are very common with report-based methodologies for detection, which focus on looking at simple metrics that cast a wide net, but often have reasonable explanations upon deeper investigation.

Number of Cases Reviewed

A reasonable measure of a team's capacity and workflow efficiency is the number of cases reviewed in a given month. A "case" may have a variety of definitions, but it is traditionally defined as an event that has some degree of suspiciousness to it that is investigated, documented, and provided with some resolution state (violation, inconclusive, not violation, etc.). Increasing the number of cases reviewed can be either a good or bad thing, depending on the proportion of them that end up being true violations.

Time Spent per Case

This critical metric is currently at troubling levels for many health systems. Many health systems report spending dozens of hours to resolve complex cases, between reviewing reports, gathering data, making requests from different departments for resources, and ultimately writing up reports. Driving improvement in these statistics not only allows diversion teams to focus on more strategic goals, but also speeds time to resolution, another key KPI with safety implications.

Workflow Efficiency

Workflow efficiency is the number of "touches" to a case that have to occur before it can be resolved. The more individuals need to review the case in order to resolve it, the less efficient the workflow.

Workforce Repeat Offense Rate

This is the rate of individuals who repeat a given offense. The measure evaluates whether interventions and education are working.

§ 6.08 CONCLUSION

We hope that this chapter has provided some insights into the possibilities of HCA and helped empower you to understand what to consider in implementing such a system or set of systems, as well as how to measure the success of your program in this paradigm. While still new, world-leading institutions have been highly successful in pursuing an analytics-driven program to reduce risk across their organizations through next-generation insight. As this paradigm becomes increasingly prevalent, new resources, approaches and tools continue to empower its rise in the industry.