While moving patient health records from paper files to electronic data has created increased complexities and concerns for protected health information (PHI) security, the move has already yielded several benefits and promises to yield many more. Electronic health records (EHRs) make it easier for clinicians to share data with one another, which helps improve treatment, reduce duplication of services, avoid medication conflicts, and deliver other benefits. It has also given rise to the field of healthcare informatics, which uses large quantities of data to help providers manage the health and wellness of populations while improving patient safety and satisfaction as well as lowering the cost. Electronic data has been a game-changer in nearly every aspect in the field of healthcare.

Yet the aspects that have made all of this progress possible have also created new vulnerabilities. Obtaining unauthorized access to confidential patient health information from patient records used to mean physically breaking into a physician’s office or hospital file room; now it can be done from anywhere in the world with a basic computer, Internet access, and a measure of determination. As the “bring your own device”
(BYOD) trend grows among healthcare professionals, gaining access to PHI is sometimes as simple as stealing a smartphone left sitting unattended.

Recent incidents, such as the [2015 breach of tens of millions of member records at Anthem Inc.](https://www.anthem.com), demonstrate that the threat is very real. Yet not all issues must be large-scale in order to create headaches for healthcare organizations. Something as simple as an employee gaining unauthorized access to a celebrity patient’s PHI and sharing it through their social media network (or selling it to the tabloids) can create a violation of the [Health Insurance Portability and Accountability Act](https://www.hipaasolutions.com/hipaa-basics/) (HIPAA). The result can be stiff financial penalties for the provider as well as tarnishing its reputation.

**PROTECTING PHI: ACCESS AUDIT TRAILS AND SECURITY**

Ensuring PHI is properly protected in the digital age falls into two distinct areas. One is the ability to audit who accesses the data and what they do with it. Having an audit trail is required by HIPAA, although the degree of granularity kept in the logs can vary by what the organization deems to be useful. Patients also have the right to request additional protection for their information, so the system used for auditing access must be flexible enough to take that into account as well.

The second is the ability to control who has access to the data in the data warehouse, which falls under security. A strong, multi-tiered security mechanism is critical to preventing unauthorized access to the data warehouse from within as well as outside the organization. It must enable the organization to control who has access to which data based on their role (need to know), down to the column or row level, to ensure that the data is useful to the organization without compromising patient privacy.

Health Catalyst has incorporated leading-edge auditing and security technologies into our [Late-Binding™ enterprise data warehouse](https://www.healthcatalyst.com/products-and-solutions/late-binding-enterprise-data-warehouse) (EDW) to address these issues. This white paper will discuss the current risk state and how Health Catalyst is addressing the challenges around it.

**UNDERSTANDING AUDITING REQUIREMENTS**

Patients have the right under HIPAA to request disclosure of who has accessed their PHI, which means providers are responsible for tracking that information.

Currently, the organization doesn’t have to provide the information down to the individual level if the access is to carry out treatment, payment, or operations (such as a clinician providing care or someone in finance preparing billing). It must only show the organization accessed the PHI. If the information has been
shared with a third party such as a Business Associate, or is part of mandatory reporting to state and local agencies, that information must also be included in the disclosure. Again, this is by organization, not individual.

That may change, however. The Office of the National Coordinator for Health IT’s (ONC) Privacy & Security Tiger Team, a workgroup established to review current policies, has recommended two new “addressable” standards be added to the HIPAA security rule. The recommended audit controls include logging granular ePHI access activities to the individual level and ensuring that the audit information supports individual activity review and inappropriate access investigation. Tracking PHI access to that level of granularity may require an extensive investment in audit data logging and storage, as well as application development and implementation. The Health Catalyst EDW already allows this level of granular audit logging.

AUTHORIZED DISCLOSURE OF PHI

Patients also have the right under HIPAA to refuse having their PHI shared with other providers or organizations, or to restrict the level to which it is shared. For example, a patient with HIV may not want that information shared with their county agency for fear that a poorly secured system will cause it to be exposed and create problems for them at work or in the community. Physicians cannot even share PHI with other physicians unless the patient consents to it. Concerns over confidential information could cause the patient to request disclosure; the provider must then produce documentation that shows it has been following the patient’s wishes.

Regardless of the circumstances, all of the above would be considered instances of authorized disclosure of PHI, because there is a legitimate reason for those individuals or organizations to view it. There is another aspect that must considered, however, and that is unauthorized disclosure of PHI.

UNAUTHORIZED DISCLOSURE OF PHI

Unauthorized disclosure occurs when someone who has no reason to view the data views it anyway. It could be an instance of an employee who is not involved with treating a celebrity looking into the celebrity’s confidential health record. It could be accidental, such as sending a patient’s records to the wrong doctor, or to a local auto repair shop with a fax number similar to the correct doctor.

Whatever the reason, unauthorized disclosure is a violation of the patient’s rights under HIPAA and must be documented as part of the organization’s auditing capabilities. Whether it needs to be reported to the Department of Health and Human Services (HHS)
depends on the circumstances. In the case of accessing celebrity records or faxing the information to the repair shop, the answer is yes. If the data was sent to the wrong medical professional who protects the data according to HIPAA, securely deletes it and lets the originating healthcare organization know about the mistake, it does not have to be reported. The same is true if a non-HIPAA-compliant third party can prove that the PHI was never opened or viewed. This can occur if the PHI was sent via email, for example, and the email is deleted without being opened.

No matter whether disclosure was authorized or unauthorized, or must be reported or not, the healthcare organization is responsible for documenting it. The key to meeting HIPAA requirements is implementing auditing technology in the EDW that automates the data logging process, provides PHI monitoring at multiple levels, includes reporting functions that help organizations improve PHI monitoring over time, and has enough flexibility to make adjustments to meet future regulations. The Health Catalyst EDW auditing solution has been created to meet all of those needs.

HEALTH CATALYST APPROACH TO EDW AUDITING

Health Catalyst focused primarily on two areas in creating our HIPAA-compliant auditing solution:

- Enabling healthcare organizations to specify the right balance between having enough granularity of information to meet their specific requirements and the cost to provide that information
- Making it easy to filter and view the audit data in a way that is meaningful to the organization

The Health Catalyst solution is reactive, providing a way to look at each action taken and each change that occurs. For example, if a user quits and the organization wants to see which PHI he or she has been accessing, the Health Catalyst system can provide a retrospective view of the systems that were accessed and which data were viewed by that user.

The organization can determine which parameters are meaningful and which can be ignored when setting up the auditing system. The platform is configurable on different levels, and can get granular down to the individual user level, or to the patient record on the data side. The result is the organization can see that John B. accessed records as well as which records he accessed. It is up to the organization to determine, however, how detailed it wants to be at each level.
IDERA COMPLIANCE MANAGER MONITORS ACTIONS ON THE DATABASE

Health Catalyst installs an Idera Compliance Manager agent on each of the SQL servers to monitor the SQL databases that make up the EDW and logs each event. It resides on the back end—the furthest point from the user—monitoring actions such as which user account did a select and then queried or changed certain data elements, or inserted data into the database.

The agents are configurable so the organization can get as granular as it wants in logging data. That said, Health Catalyst typically advises clients to exercise caution in determining how much data to log at the database level to avoid having the cost out-strip the value. The amount of space required to store that data could be larger than the space needed for the data itself if an organization chooses to log every step. And most of the logging data will never be used. Too much log data could also have a negative effect on application performance and is often never used. The key is to capture all the information that’s significant without getting bogged down in the minutia. Health Catalyst generally recommends logging at a minimum the data set that includes:

- Who inserts data into the database
- Who logs in to access the database
- Who has been trying to log in but failed; that could be the result of an error in typing the password or use of the wrong password, but it could also be someone attempting to use credentials that are not their own

Our goal is to help clients capture everything that is significant without getting caught up in the trivial, but in the end the decision of how to configure the Idera database agents is theirs.

A central management console aggregates data from all the individual agents into an audit data repository to make it easy to drill down into the data and view specific events. A reporting tool with graphical representations enables administrators and compliance officers to use the data to spot trends and ensure that any weaknesses are strengthened quickly.

QLIKVIEW TO MONITOR USERS

Health Catalyst uses QlikView logs to help monitor user activity on the visualization side (the part of the process that is closest to the user). QlikView is like a browser, allowing users to search the database for specific types of data.
The QlikView logs allow administrators and compliance officers to see which data was searched, and what types of filters were used, to determine whether PHI was included in the search. As a result, if a user searches for everyone in the database who is HIV-positive, that information will show up in the QlikView log. This information will help administrators and compliance officers spot users who are attempting to gain access to data not related to their job functions.

**PLATFORM AUDITS – A HEALTH CATALYST EXCLUSIVE**

Between the user and the database is what we call the platform layer, which sits on top of the databases. This is unique to Health Catalyst, and a function of our Late-Binding enterprise data warehouse (EDW) technology. The EDW takes data from all of a healthcare organization’s disparate sources, no matter what form it’s in, then converts and stores it in a format that can be used to create analytics and visualizations from a single system.

Since most queries run on an EDW are population based, they may contain hundreds, thousands, or even millions of results. The platform audit logs track metadata about these queries. For example, the audit log would contain the date and time, username, source computer, program used and the query text.

The result is three layers of auditing that create a comprehensive audit trail for health data to protect the organization in the event a patient wants to know who has been viewing their PHI, and to what extent.

**SECURITY AND THE VALUE OF PHI**

The recent increase in the targeting of PHI is the result of the high value this information brings. According to cybercrime experts, stolen PHI is 10 times more valuable than credit card information. While credit card numbers can be used to purchase expensive items, that is all they can really do. They are also generally identified as soon as they are used as most credit card companies have departments dedicated to detecting and reacting quickly to potential fraud.

The data contained in PHI, on the other hand, can be used to generate identities, obtain health services, submit false insurance claims, order pharmaceuticals, and perform other illegal acts. This activity can go on for months before being detected due to the methods being used and a lack of focus on fraud detection throughout the healthcare industry. That is why data security has become of paramount importance to healthcare organizations.
DETERMINING HOW SECURE

Before we get into the specifics of the Health Catalyst approach to data security, it is important to point out that just as it is possible for data to not be secure enough, it is also possible for it to be too secure. The goal is to strike a balance between preventing unauthorized access to data and giving users what they need to do their jobs effectively.

Analytics rely on data; in order for the organization to make clinical quality and other improvements, analysts must have the right access to the right data. At the same time, the more people who are given access to data, the larger the attack surface gets. If only one person has access to the data it is easy to keep tabs on that user. If 1,000 people have access to the data, however, the organization must watch over 1,000 people—and cybercriminals have 999 more targets.

That is important because despite Hollywood’s portrayal of hackers sitting behind computers attempting to break complex encryption codes in order to gain access to a network, social engineering techniques such as phishing (attempting to obtain logins and passwords through techniques such as an email that appears to be from a trusted friend) are the more likely path of entry.

In the last few years, the situation has gotten even more complex thanks to social media and the general availability of information on each of us. Armed with just a name, cybercriminals can scour Facebook pages, Twitter feeds, sites such as Ancestry.com, Google street view, and more to learn the names of employees’ spouses, children, parents, and other relatives, discover their hobbies and interests, see what grade school they went to, learn what type of cars they drive, the color of their houses, etc. They can then use all of that information to convince employees they have a message from a friend, and try to get those employees to take an action that ultimately gives them access to the organization’s most closely-guarded information. Especially if the organization has not taken adequate steps to protect it.

A lack of adequate protection is typically the norm. Healthcare providers traditionally have not been in a position to devote the time or resources to hardening their internal security for a variety of reasons, not the least of which is the need to comply with government-mandated programs such as EHR implementation. This leaves them more vulnerable to cybercrime than comparably-sized organizations in other industries. Couple that with the fact that cybercriminals can devote 100 percent of their time and resources to breaking healthcare organizations’ security (sometimes with the backing of foreign governments) and the risk increases greatly.
One way to address this issue is to implement an EDW that already has extensive auditing and security capabilities built into it. That is what Health Catalyst offers.

HEALTH CATALYST APPROACH TO EDW SECURITY

Health Catalyst offers two options for the solutions packages that enable users to leverage the EDW to create visualizations.

One is to license the analytics software and install it in their network. This option gives the organization total internal control over security and compliance. The second is to host the solutions package in the Health Catalyst data center, creating a secure VPN connection between the health organization’s environment, and Health Catalyst. Both offer extensive, multi-layer approaches to security.

PHYSICAL AND ENVIRONMENTAL SECURITY

For clients who select Health Catalyst’s hosted solution, we have our own equipment co-located in a Tier 3-certified data center facility that meets all the best practices and industry standards for environmental and physical controls. We maintain our own servers, firewalls, storage area network (SAN), and other technology within that facility. Entering the building requires scanning a badge and biometric palm print identification. Once inside, a floor-to-ceiling cage that also requires scanning a badge and thumbprint identification to enter protects access to Health Catalyst servers. This secured cage is video monitored 24/7 with recordings available for review as required.

From an environmental standpoint, the Health Catalyst data center includes redundant power and cooling capabilities.

Health Catalyst creates a distinct Virtual Local Area Network (VLAN) for each client that selects a hosted solution. That client environment is logically separated from every other client environment in order to prevent one client from accidentally accessing the data of another. There is no lateral network traffic across client environments.

PLATFORM SECURITY

The platform allows administrators to flag individual columns or records in a database as to whether the information they contain is:

- Not sensitive – general information such as the state or a patient’s gender.
- Sensitive – personally identifiable information such as name, date of birth, or a Social Security number.
PHI – these are the 18 data elements covered under HIPAA that must be de-identified before being passed along for research. The organization must be able to ensure that the individual cannot be re-identified using that data set.

The data can be flagged to prevent it from being viewed or used in visualizations by users who do not have the proper permissions in the EDW. Flagging sensitive/personally identifiable and PHI data in the platform bridges the gap between the user browser level and the database.

DATA STEWARD MODULE

This is an important component of the Health Catalyst security offering because it helps the healthcare organization maintain control over the data more effectively.

Analysts may see that the organization holds a certain type of data because they can see the column names, but they cannot see the actual data itself. If they want to view the data, they must put in a request to the data steward, who will decide whether or not to allow access. The data steward in coordination with the EDW administrator can create custom database views to meet the analyst’s requirements.

The advantage of the data steward model is that control over access to sensitive data is kept in the hands of a user with intimate knowledge of the data as well as the organization’s standards for use. Health Catalyst’s data steward module ensures there is a workflow in place for identifying who the data steward is for each area and that requests to view data are processed efficiently.

IDENTIFICATION AND AUTHORIZATION

Health Catalyst uses Microsoft Active Directory identification and authorization database to enable role-based security within the EDW. Active Directory provides very granular control over who can and cannot access a health system’s data, its EDW, and the various applications. Health Catalyst defines the roles, and then it is up to the client to assign and manage those roles for each of the users whether the client is using an on-premise or hosted solution.

Health Catalyst typically recommends creating the following database roles that can be used to manage access:

- **Data Readers** – this role normally consists of data analysts who only need to view data. This role can be granted access to specific databases while restricting access to others.
Data Writers – this role normally consists of power users, who in addition to viewing data need the ability to insert, update, and delete data.

Data Loaders – this role is typically reserved for service accounts that load data into the EDW from the source systems.

Data Developers – this role is granted to users in the development environments, which allows them to perform tasks including: managing and creating tables, procedures, functions and schemas.

EDW Operators – this is a server level role, which allows users to create automated jobs and monitor the performance of the EDW.

Each of these roles, with the exception of EDW Operators, is configurable at the database level so that databases containing sensitive data can be configured accordingly.

The idea, which follows industry best practices, is to give each type of user the least amount of privileges required to perform their jobs effectively.

Clients always have the ability to make granular adjustments to these roles, or to create a new role if one becomes necessary. For example, people in a particular role may need to have access to a patient’s date of birth, which is personally identifiable sensitive data, but not other sensitive data such as whether the patient is diabetic if that is irrelevant to the analytics being performed. The client’s system administrators can create a role that enables that level of access, even if that role only applies to one person.

System administrators can lock users out of particular columns by default, then provide access to those columns based on a particular need. They can also do this at the row level to prevent access to specific records, such as those of a celebrity, if desired.

This platform security is embedded into the operating system and database management system supporting the EDW. The system provides the means for associating the user names of the people logging into the EDW with their authorized levels of access to the data content and visualization applications. As discussed earlier, the access control system also provides an audit trail for tracking who accessed which data and when.

AUDITING AND SECURITY COMPLIANCE FOR PHI IS CRITICAL

The ability to show who is using that data (and how they’re using it), as well as protect it from falling into the wrong hands, grows exponentially as...
healthcare organizations become more reliant on data and analytics. Yet building those capabilities internally to a level that meets HIPAA compliance requirements and follows security industry best practices is often beyond the reach of hospitals and health systems given the many other high-priority technology projects commanding attention from IT. Which means those organizations must acquire them another way.

When looking at working with an outside vendor for auditing, healthcare organizations should focus on how granular they can get, how easy it is to view audit data and filter it in a way that is meaningful to the individual requesting it and whether the vendor’s technology fully meets all HIPAA requirements. For security, again the organization will want to look at how granular it can get, whether the system supports the concept of the least privilege required to get the job done well, and whether the security roles meet Health Information Technology for Economic and Clinical Health (HITECH) security rules under HIPAA.

These HIPAA-compliant best practices for auditing and security are already integral components of Health Catalyst’s Late-Binding EDW. Which means as an organization builds its data and analytics infrastructure, it’s also building the capabilities to protect PHI and other sensitive data. And protect itself.

When looking at working with an outside vendor for auditing, healthcare organizations should focus on how granular they can get, how easy it is to view audit data and filter it in a way that is meaningful to the individual requesting it and whether the vendor’s technology fully meets all HIPAA requirements.

Bob White, Director Security & Compliance

ABOUT HEALTH CATALYST

Health Catalyst is a mission-driven data warehousing, analytics, and outcomes improvement company that helps healthcare organizations of all sizes perform the clinical, financial, and operational reporting and analysis needed for population health and accountable care. Our proven enterprise data warehouse (EDW) and analytics platform helps improve quality, add efficiency and lower costs in support of more than 50 million patients for organizations ranging from the largest US health system to forward-thinking physician practices.

For more information, visit www.healthcatalyst.com, and follow us on Twitter, LinkedIn, and Facebook.