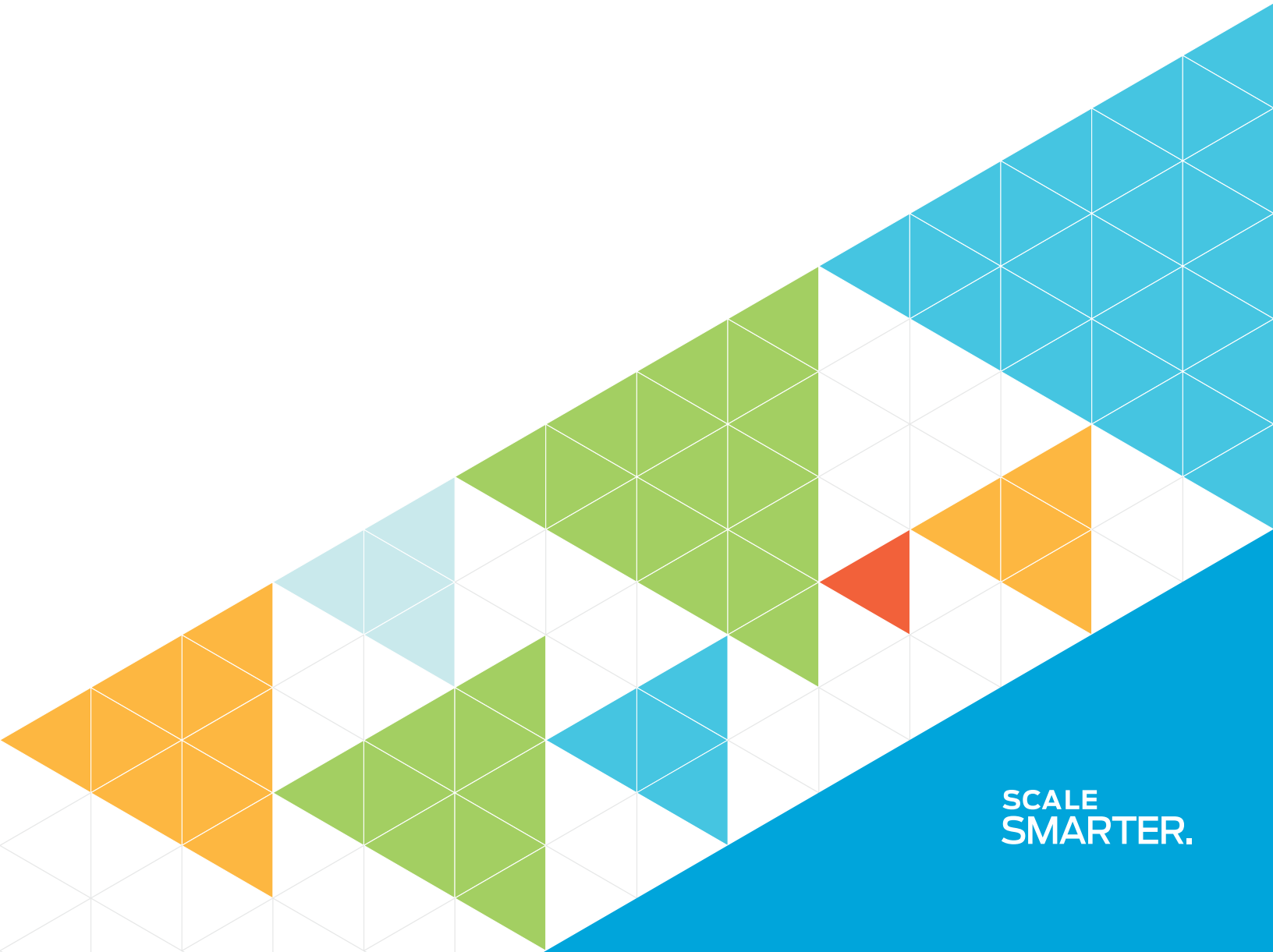
Corepoint HEALTH

Improve PHI security using a modern interface engine



Data breaches and HIPAA violations come in all forms. Those most likely to make the news involve a hack from outside sources and hundreds of thousands of missing patient records. As CIOs know, there are many PHI breaches that can occur daily that involve only a handful of patient records. These "minor" violations have as much potential to violate a patient's rights and harm the reputation of the hospital as any breach that makes the daily news.

Take, for example, when a celebrity is admitted to the hospital. Data security and patient privacy is of utmost importance when a great majority of hospital staff are interested in the details about the celebrity so they can be the first to break the gossip to their friends and even to the media. However, unless the caregivers are assigned to the patient's caregiving team, it is against HIPAA rules for hospital employees to access an individual's health record, let alone post that information to the Internet.

A patient such as a celebrity or a politician must have the same rights to privacy as every other patient at the hospital. It is the responsibility of the administration to put the proper safeguards in place to protect the patient.

One helpful safeguard is the organization's interface engine. If it is the data within the patient's health record that is of interest, what better place to look to see who has accessed PHI, what portions of the record they viewed, and what actions were taken with the data than the software responsible for routing the data from application to application?

Audit Logging and Log Search, two features in Corepoint Integration Engine, provide key insights into your organization's health data, beginning at its origin through its route through every interface in your health data architecture.

Audit logging

Audit logging has long been a required functionality for EHRs. Backend applications historically have gotten a get-out-of-jail free card with regards to audit logging. The perception is that the software is kept secure to data room servers, where access is limited to IT personnel only. These IT personnel are trusted individuals who have administrative rights to roam among sensitive data regardless.

Modern integration engines, however, provide features that extend outside the secured IT datacenter. Integration engines now extend into departments, allowing technicians to view, monitor, and debug message flow themselves. This empowers departments with the necessary tools to get data flowing again during interruptions, without being so dependent on the interface team.

This departmental access makes it critical that an interface engine incorporates the same audit logging capabilities as an EHR into the product. Tracking of any PHI exposure is critical and a requirement of Meaningful Use.

Corepoint Integration Engine's Audit Logging provides:

- The ability to log events such as:
  - Additions
  - Deletions
  - Changes
  - Queries
  - Printing
  - Copying
- The ability to log pertinent data such as:
  - Date and time of event
  - Patient identification
  - User identification
  - Type of action (from the list above)
  - Identification of data (such as labs, demographic, etc.)
- Audit logging by default
- Tamper-resistant data storage
- Ability to generate reports

Corepoint Integration Engine has modeled its audit logging requirements after the Meaningful Use definitions, and has passed the criteria for the 2014 Edition for EHR technologies.

Log search

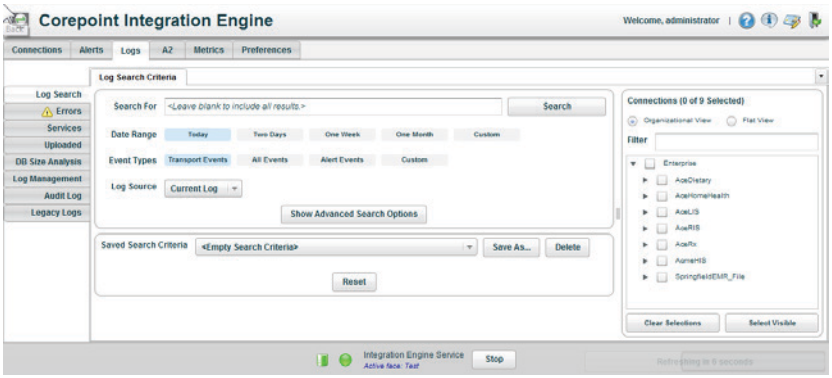
Corepoint Integration Engine allows users to perform simple and advanced Google-like message searches across multiple connections, which provides the complete history of a message directly in the Log Search window. Search criteria can be modified from those results to further narrow or broaden the search to provide key insights about the message's lineage.

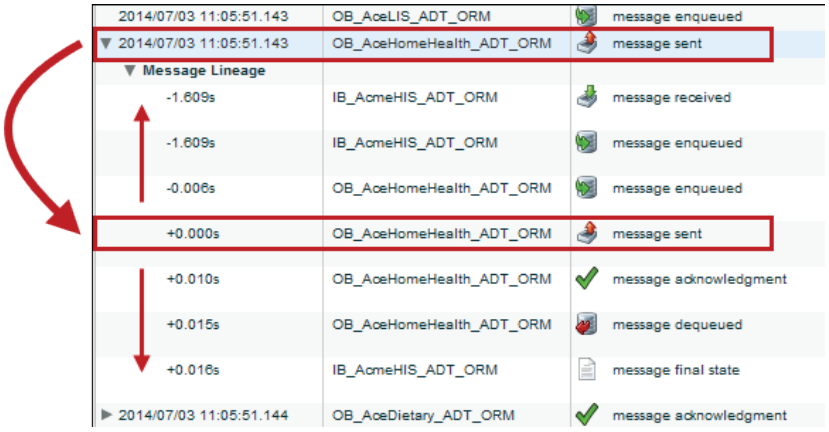
Conduct a search of all connections with no applied filters to display all connection log information on the Search Results tab. Enter specific search data, define a date range, and select specific event types to narrow the results.

From the search results, users can expand a message to view its complete history as it progressed through Corepoint Integration Engine. This is valuable for security because it can help trace a message if a breach or violation occurred downstream with trading partners. It also provides valuable information such as why messages are not showing up at a specific trading partner, why a trading partner is rejecting a message, or why other applications are sending a particular message code.

In addition to providing valuable information that can be used to improve security, Log Search also provides:

- **Errors tab** Quickly search and manage your error logs separate from the main Log Search view. A warning indicator alerts you to errors for the current day.
- **DB Size Analysis** View database size and free disk space information for each log database, down to each connection.
- **Log Management** Create archive databases to move log data from the managed log database to an archive to free up space or to meet long-term storage requirements.
- **Legacy Logs** Complex filter sets can be saved and used for future log searches.





With the need to share more PHI, it is imperative that health care providers have access to the granular details about their patients' data flow. In addition to unparalleled performance and support, Corepoint Integration Engine provides functions that empower your IT team to scale smarter with the added confidence that data security can be simultaneously strengthened.

Follow us

Twitter.com/CorepointHealth

Facebook.com/CorepointHealth

Plus.google.com/+Corepointhealth

Linkedin.com/company/Corepoint-Health

Blog (corepointhealth.com/GENi)