Health System Significantly Improves Privacy Incident Reporting Capabilities

Inadequate and inaccessible privacy investigation data was compromising analysis and decision-making for the compliance department of a major health system. Compliance leaders were forced to make do with incomplete input from an archaic data log and reporting system.

Problem to Solve

In health care, decision-making without sufficiently clear and accurate data is a recipe for poor choices and costly mistakes.

Inadequate and inaccessible privacy investigation data was compromising analysis and decision-making for the compliance department of a major health system. This was a significant concern as this organization serves more than a quarter-million patients annually.

Instead of being able to access sufficient data for internal reports and presentations to the health system's executive leadership, compliance leaders were forced to make do with incomplete input from an archaic data log and reporting system. This potentially impaired the ability of executive leaders to understand and act on compliance information.

Rather than continuing with an outdated data system and processes that no longer met the health system's needs, the compliance department engaged Freed Associates (Freed) to improve its privacy investigation methodology and dashboard and reporting capabilities. These improvements were needed to ensure the organization is

properly handling privacy incidents, reduce its potential risk exposure and the chance and expense of privacy-related litigation, and be prepared for any external audit of compliance records.

Strategy and Tactics

Freed began the engagement with a rapid series of subject matter expert meetings to discuss and determine the deficiencies of the department's current privacy incident log versus the department's desired reporting requirements. These meetings revealed several opportunities for improving the department's handling of privacy investigations, including:

- Developing a privacy investigation team (PIT) escalation framework with a corresponding customized slide deck for PIT committee meetings
- Identifying measurable privacy breach information available for capture, based on current department workflow, content and reporting needs
- Redesigning the existing privacy incident log fields and creating new log fields to capture previously unavailable data
- Migrating the privacy incident log from a shared drive to secure cloud storage, allowing multi-user access and editing
- Developing and enhancing key performance indicator (KPI) documentation
- Developing analytics reporting capability using software with KPI documentation

Client input for improving the PIT escalation framework, privacy incident log redesign, and reporting capability was incremental, as staff members regularly noted ongoing opportunities to tweak and/or add to these tools. This was a positive, as it meant that these tools would be tailored to the specific needs of the compliance department and health system.

Results

The client was able to achieve all of its desired privacy incident log improvements. These results included:

- **Created 15+ new sustainable and measurable privacy incident log data fields** to help the PIT and department leadership better present privacy incident-related reports
- **Improved reporting capabilities with a suite of 16 new dashboards,** allowing both department and health system leadership to more easily see and understand privacy incident trend information and make corresponding operational decisions as needed
- **Improved staff member teamwork and efficiency by migrating data input and access from a shared drive to a cloud environment**, allowing more than one person at a time to edit data
- **Improved the adaptability of data fields,** allowing them to be updated, depending on new business needs

- **Added analytics reporting capability,** providing department leaders with a clearer and more actionable means of analyzing and presenting privacy incident-related data

Throughout this engagement, the client was reminded to plan for ongoing maintenance and sustainability of these new and enhanced privacy incident data tools, to ensure their ongoing relevance and usefulness.

Conclusion

By taking these important steps to improve its data system and processes, the compliance department significantly enhanced the health system's ability to handle privacy-related incidents. This, in turn, reduces the health system's risk exposure, minimizing the chance, time and expense of any privacy-related litigation and better-preparing the organization for an external audit of its compliance records.

Overall, this work illustrates the value of improving data quality and accessibility within any data-dependent health care department, and particularly so within compliance.

