SailPoint

SOLUTION BRIEF

Securing Data in Educational Institutions

An estimated 80 percent of all the data in the world is stored in files. Often times, these files reside in less secure locations outside a database or application. Many colleges and universities have no visibility into where these files reside, what each file contains, and who can access this data. For educational institutions managing sensitive content related to proprietary research, personal identifiable information (PII), protected health records (PHI), payment card industry (PCI) and other sensitive material, this creates significant cybersecurity vulnerabilities and risk that cannot be ignored.

If you don't know where sensitive data resides, you cannot protect it. For this reason, institutions need identity governance capabilities that extend beyond databases and applications.

Understanding the Data Lifecycle

Educational institutions typically have hundreds of systems and applications containing sensitive data. The collaboration and sharing of information is every bit as essential to students as it is to employees and contractors. But maintaining an open culture can create blind spots where sensitive data is not well protected. One of the most significant examples of this occurs when sensitive data is exported from these systems and applications.

For instance, an administrator compiling a report on the student population may access sensitive data from the HR system, learning management system (LMS) and even clinical systems. This staff member may export the information into an Excel file as part of the workflow. Similarly, a faculty member doing research may pull sensitive data that is flowed into a Word or PDF document for a white paper. Where are these files stored? Typically, the data turns up in a variety of places like network file shares, SharePoint and cloud drives. These locations are typically vulnerable to exposing sensitive data to prying eyes.

Three Steps for Securing Files with PII, PCI, PHI and Other Sensitive Data

Once you understand the challenges associated with governing data within an education institution, you can begin to build a game plan for securing it.

FERPA and HIPAA have very specific rules defining what type of information and/or combination of information needs to be protected. It also defines significant financial consequences for failing to secure that information from unauthorized access by individuals or groups. Violating FERPA rules can expose schools to lawsuits and loss of federal funds. With HIPAA, universities can be fined up to $1.5 million per violation per year. For these reasons, educational institutions would be wise to track down and govern access to any files containing PII, PCI and PHI. Here are three essential steps for securing sensitive data.

Step 1

Discover and Prioritize: The amount of sensitive data stored in files is growing at an exponential rate. Just locating data files, much less managing access to that information, can be overwhelming. To streamline efforts and minimize impact on IT resources, a targeted approach is far more reasonable and achievable. Rather than boiling the ocean, educational institutions should conduct a comprehensive audit and flag files that contain sensitive content. This enables them to prioritize efforts and exercise precision in securing FERPA- and HIPAA-related content and other sensitive data.

80%

of all data is located in digital files across educational institutions, making it essential to exercise precision in governing access to the most sensitive data.

Step 2

Assess Who and What: Analyze who should have access to what data. To control and govern access to sensitive information, it is critical to build out a model that correctly identifies users who have justification to access specific types of sensitive data. Education institutions will want the ability to automatically compare the actual state-of-access with the desired state, and eliminate over-entitled users on a regular basis. This can be formed through regular access review processes or more automated reconciliation tasks. This assessment will help set the foundation of critical governing policies moving forward.

Step 3

Empower Data Stewards: Who in the institution would have the best understanding of which users should have access to what and when? While IT departments often end up with the responsibility, they rarely know the data or the users. On the other hand, data stewards have contextual understanding of the data and users. For these reasons, it is essential that education institutions determine and designate data stewards.

As you set policies around access, it's important to ensure the processes for granting and validating access are conducive for the desired security results, while minimizing impediments to the users' day-to-day operations.

SailPoint's Advantage

SailPoint helps educational institutions eliminate cybersecurity and compliance risks with a comprehensive identity governance solution that applies to all data, wherever the information resides. Our approach streamlines the process for finding sensitive information in files and documents located throughout the school or education system. We further enable IT administrators and data owners to prioritize and focus on managing content that poses the greatest regulatory compliance and cybersecurity risks.

Moreover, SailPoint is recognized by Gartner and Forrester as the leading authority in identity governance and administration. This is essential because knowing and governing identities is a central tenet to protecting sensitive information and ensuring reasonable freedom of access for those who legitimately require information as part of their daily workflow.

Benefits to Educational Institution

Enhance visibility into FERPA- and HIPAA-related content and other sensitive data

- Locate and classify sensitive data based on content or who is accessing data
- Support more intelligent governance decisions with deeper insight about users and access that provide complete identity context
- Monitor on-premises and cloud data access in real-time

Drive compliance with corporate and regulatory requirements

- Help drive compliance with proven policies, rules and search expressions
- Streamline access reviews and certifications to quickly respond to audits and maintain compliance
- Maintain a real-time health status across all governed data sources and take action on potential compliance risks

Establish governance control with business accountability

- Utilize targeted crowd-sourcing to more accurately identify owners responsible for sensitive data
- Ensure only authorized users (defined by HR, IdentityIQ/IdentityNow or role modeling) are provided access with streamlined access requests
- Detect and respond to policy violations in real-time with automated alerts

Remediate risk with actionable intelligence

- Enable IT, security and business users to identify and remediate risk with actionable dashboards
- Address permissions creep and establish one permission path per user with access normalization and cleanup
- Avoid human errors while reducing IT workload with automated access fulfillment

If you are interested in learning how our solutions can help your institution locate, secure and manage sensitive data and files, **contact us** to set up a demonstration.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies.