How Sanction Screening Supports Patient Data Security

Over 500 million Americans' healthcare data has been breached since 2009, with the number rising steadily in recent years. Protecting patient data is a growing challenge for healthcare organizations, requiring a multifaceted approach to address both internal and external risks.

One important factor in improving patient data security is the introduction of more comprehensive sanction screening. While not a standalone solution, sanction screening plays a key role in reducing risks by identifying high-risk individuals or entities. This article explores exactly how and why sanction screening supports better patient data security.

Protecting Patient Data: An Overview

Why is it Important to Protect Patient Data?

Protected health information (PHI) is highly sensitive and strictly regulated worldwide. The reason is simple: in the wrong hands, it can be highly damaging to the affected individuals. A few examples include:

- **Identity Theft**: PHI is a frequent target for identity thieves, with studies estimating that 70% of all PHI can be exploited for fraudulent activities. These include financial fraud, stolen medical insurance, or the creation of fake IDs.
- **Blackmail:** Individuals may be blackmailed by criminals under threat of revealing sensitive health information to their friends, colleagues, or employers.
- **Targeted Marketing:** Private information about an individual's health status could be weaponized to deliver target marketing messages that the individual is particularly vulnerable toward.

This has created a huge black market for patient data, leading healthcare to be both the industry most heavily targeted by cybercriminals and the most extensively regulated with regard to data privacy.

Key Regulations Related to Patient Data

At the federal level, there are two primary regulations in the US that govern the protection of patient data:

- **HIPAA:** The Health Insurance Portability and Accountability Act (HIPAA) provides a set of national standards for the protection of patient data privacy and security. It comprises three core rules - the Privacy, Security, and Notification Breach Rules – and can lead to non-compliance fines of up to an estimated $2 million **per violation category, including criminal prosecution.**
- **HITECH Act:** The Health Information Technology for Economic and Clinical Health Act (HITECH) was passed in 2009 to promote the adoption of electronic health records (EHRs). However, it also introduced additional support to existing HIPAA measures, such as requiring covered entities to report data breaches that affected 500 or more patients to the news media.

Together, these regulations require healthcare entities to implement extensive data protections, such as:

- **HIPAA Safeguards:** Technical, administrative, and physical safeguards to ensure PHI is never accessed by unauthorized individuals
- **Privacy Training:** Employees must be given frequent training to ensure they know how to handle PHI appropriately, prevent unauthorized access, and respond to potential privacy breaches.
- **Regular SRAs**: Security risk assessments (SRAs) must be undertaken regularly to ensure patient data is secure and hidden cybersecurity vulnerabilities are not easily exploitable.

While privacy and security measures are paramount, another important yet often overlooked compliance tool is sanction screening.

3 Ways Sanction Screening Helps Protect Patient Data

Sanction screening is a formal process designed to assess whether healthcare providers, employees, contractors, vendors, or entities are listed on government or regulatory exclusion lists. This has several important implications for patient data safety:

1. Minimizes Fraud Risks

Insider attacks, where an employee intentionally accesses or steals patient data, are surprisingly common, with the healthcare industry experiencing more of these attacks than any other industry. While excluded individuals are not the *only* potential perpetrators, they can be reasonably considered a higher risk.

Sanction screening reduces the likelihood of introducing high-risk individuals into your organization, thereby lowering the potential for insider attacks. These measures **demonstrate that your organization is taking reasonable steps to vet individuals and reduce insider threats, which can** support your case **for** due diligence in the event of a breach or compliance review, potentially mitigating HIPAA **penalties**.

2. Reduces Third-Party Risk

The single most common cause of healthcare data breaches is third-party vendors. The average healthcare organization uses a vast network of external partners for everything from supply chain management to electronic healthcare record (EHR) software. These vendors are often given access to the entity's IT system, which means a cybercriminal that infiltrates the vendor could easily gain access to your patient data.

Regular sanction screening helps to monitor and proactively vet vendor behavior more effectively. By identifying those with compliance issues or past misconduct, it reduces the likelihood of partnering with vendors that could expose your organization to security vulnerabilities or regulatory risks. While not a substitute for broader cybersecurity measures, it adds an important layer of due diligence.

3. Builds a Culture of Compliance

Patient data protection and security affects every member of your workforce – even those who do not directly access data on a regular basis. Building a culture that prizes compliance and data protection is vital to ensuring every individual consistently follows best practices.

Sanction screening reinforces a culture of compliance by demonstrating your organization's commitment to ethical practices and patient data protection. It sends a clear message that safeguarding sensitive information is a priority, encouraging employees and partners to uphold high standards in their roles. The question then becomes: how can you effectively introduce sanction screening into your organization?

How to Introduce Sanction Screening

Sanction screening can be an intimidating process, especially when you think about scaling the process to ensure every vendor and new hire is properly vetted. However, there are four simple steps you can take to introduce and manage an efficient program:

Step 1: Identify All Relevant Exclusion Lists

To build a comprehensive sanction screening program, it is essential to begin with a clear understanding of all relevant exclusion lists. These lists identify individuals or entities prohibited from participating in federally or state-funded healthcare programs. The three key exclusion lists healthcare organizations should incorporate into their screening process as:

- **OIG List of Excluded Individuals/Entities (LEIE):** Managed by the Office of Inspector General (OIG), the LEIE is the most critical exclusion list for healthcare entities. It identifies individuals and organizations excluded from participating in federally funded healthcare programs. Due to offenses such as healthcare fraud or patient abuse. Employing or contracting with excluded parties can result in significant fines and other penalties.
- **SAM.gov Exclusions List:** Maintained by the General Services Administration, this list highlights parties excluded from participating in any federal program, including that outside healthcare.
- **State-Specific Exclusion Lists:** Some states maintain their own exclusion databases, which restrict participation in state-funded programs. These lists must also be checked, if applicable, to ensure compliance with state requirements in addition to federal regulations.

Establishing the full range of lists you will use to assess individuals and organizations will ensure your process is consistent and comprehensively screens against both federal and state exclusion criteria.

Step 2: Integrate Screening into Hiring and Vendor Processes

Sanction screening should be embedded into both **recruitment** and **vendor selection workflows**:

- **During Recruitment:** Verify all candidates—whether they're employees, contractors, or volunteers—against exclusion lists before offering a position. This ensures no excluded individuals are hired into roles involving federally funded programs or access to sensitive data.
- **For Vendors:** Screen all vendors, subcontractors, and third-party service providers to confirm they meet compliance standards and are not barred from federal healthcare participation.

Integrating these checks into hiring and procurement processes protects your organization from potential legal and financial repercussions.

Step 3: Use Automated Sanction Screening Tools

Managing sanction screening manually can quickly overwhelm even the most capable compliance teams. That's why automating the process with Compliance Resource Center's solutions is the ideal way to streamline operations and ensure accuracy.

Compliance Resource Center offers **comprehensive automated tools** that make sanction screening efficient, accurate, and scalable:

- **Real-Time Updates:** Stay ahead of compliance risks with tools that automatically sync with key exclusion lists, such as the OIG LEIE, SAM.gov, and state-specific databases. Your organization is always up to date with any changes or additions.
- **Simplified Audit Preparation:** The built-in reporting features provide detailed, easily accessible logs of all screening activities. These records simplify audit preparation and demonstrate regulatory compliance with confidence.
- **Error Reduction:** Automation significantly minimizes the risks of human error inherent in manual cross-checks, offering consistent and reliable screening results.

In addition, Compliance Resource Center's tools seamlessly integrate with existing HR, vendor management, and procurement systems, ensuring a **user-friendly and efficient workflow** for your team.

By choosing Compliance Resource Center's automated sanction screening solutions, your organization can maintain compliance with minimal effort while focusing on what matters most: delivering high-quality care and services.

Step 4: Maintain Ongoing Monitoring and Documentation

Sanction screening is not a one-time activity. Continuous monitoring and proper documentation are not only essential but reinforced by OIG guidance:

- **Ongoing Screening:** Conduct monthly checks to ensure that no individuals or entities employed or engaged with your organization are added to exclusion lists after initial screening.
- **Thorough Records:** Keep detailed documentation of all screening activities, including dates, results, and resolution of any flagged matches. This ensures your organization is prepared for internal or external audits.

Proper monitoring and documentation demonstrate your organization's commitment to compliance and serve as a safeguard against potential penalties or legal risks.

Partner with Compliance Resource Center to Keep Patient Data Safe

Are you interested in introducing more robust sanction screening but lack the resources or expertise? Compliance Resource Center offers both automated software and expert services to help you introduce, scale, and optimize your sanction screening process to protect patient data and maintain compliance.

Book a Demo