# Telehealth Compliance: Why Your Program Needs Sanction Screening Services

Nearly 40% of Americans report using telehealth in the last year, but many providers still feel their telehealth program is up in the air: how large is the compliance risk it presents? And how can it be scaled safely and securely?

This article explores those compliance questions head-on – presenting an unappreciated factor that will help enhance your program's risk management processes.

## Overview of Telehealth Compliance Challenges

### Understanding the Regulatory Landscape

Telehealth programs operate within a complex web of regulations that vary by jurisdiction. Among the most significant are:

- **HIPAA (Health Insurance Portability and Accountability Act)**: This federal law establishes rigorous standards to ensure the confidentiality, integrity, and availability of patient health information. Violations can result in penalties exceeding $1.5 million annually per violation category, as highlighted in the HHS enforcement reports.
- **Insurance Coverage:** Both private and Medicare coverage was extended during the COVID-19 pandemic, and subsequent efforts have been made to maintain this change. Bills such as the Preserving Telehealth, Hospital, and Ambulances Act and the Telehealth Modernization Act of 2024 include provisions to maintain coverage until 2026, but it is uncertain whether telehealth will continue to be available via specific health plans beyond that point.
- **Cross-Border Licensing Laws:** Telehealth providers are often required to have a license to operate in the state from which their patient calls. This varies between states, as every state has the right to allow healthcare professionals to use telehealth within their remote borders – but not all choose to do so.

But how do these regulatory requirements create friction for telehealth providers?

### 3 Key Regulatory Challenges for Telehealth

The regulations cited above present three common challenges:

1. Protecting Patient Data and Privacy

Providers must implement comprehensive policies to secure sensitive health information and comply with diverse privacy laws. A scandal broke in 2023 when one telehealth startup was found to share unauthorized data on over 3 million patients with major tech companies – and this was one of 50 telehealth companies found to be in violation of HIPAA.

2. Ensuring Proper Licensing

Telehealth practitioners must verify their credentials in every state or country where they provide services. But this creates a heavy lift for providers and can lead to significant roadblocks to service – ultimately harming patient care.

3. Verifying Eligibility and Trustworthiness

Providers need to confirm the reliability of patients, vendors, and staff, ensuring compliance and security throughout the telehealth ecosystem. Insurance fraud is common in telehealth as it is often perceived to be less risky – with recent estimates suggesting that 100 billion dollars of data security costs could be saved with better verification systems.

## How Does Sanction Screening Fit into Telehealth Compliance?

S**anction screening** is a process designed to assess whether individuals or entities are included in national and international sanctions lists. It is designed to ensure compliance with critical healthcare regulations, including HIPAA and insurance compliance requirements, by minimizing the risk of fraud and misuse of sensitive data.

An effective program can ensure your organization:

- **Avoids Financial and Legal Penalties**: Healthcare organizations risk significant fines or losing insurance coverage if they engage with sanctioned individuals or entities. The risk of doing so may be higher than normal in telehealth programs, as the individual may operate in a different state.
- **Maintains Ethical Standards:** Screening helps telehealth programs align with legal and ethical healthcare delivery practices.

**For example:** Imagine a telehealth provider inadvertently hiring a clinician listed on a sanctions registry. The consequences could include steep regulatory fines, reputational damage, and disruption of services, potentially leading to non-compliance with HIPAA's data safeguards. Implementing sanction screening would have flagged this risk – helping to preserve compliance and operational continuity.

## How to Use Sanction Screening to Improve Your Telehealth Program

Traditional sanction screening processes involve manually reviewing sanction lists. But this is unrealistic for most healthcare organizations, especially given their resource and staffing shortages – which often leads to sanction screening being overlooked or neglected.

A better approach is to implement sanction screening tools that augment human effort and ensure the process is scalable as telehealth programs expand:

### 3 Steps to Integrate a Sanction Screening Tool

1. Select a Reliable Tool

Choose a trusted sanction screening service that provides comprehensive coverage, real-time updates, and integration with existing telehealth compliance frameworks. For instance, tools offered by Compliance Resource streamline the process by automatically cross-referencing sanctions lists with provider and vendor databases.

2. Screen Regularly

Conduct routine checks on all providers, vendors, and partners to ensure ongoing compliance. Regular updates help capture any new additions to sanctions lists and reduce the risk of lapses.

3. Adapt Processes

Develop flexible protocols that can quickly incorporate changes in sanctions lists or regulatory requirements. Leveraging services like those from Compliance Resource Center allows for dynamic process adjustments that align with healthcare compliance standards.

### 3 Best Practices for Implementation

1. Automate Screening

Focus on automated solutions that enable regular screening without adding a heavy administrative burden. This will also eliminate human error and ensure consistency, especially when screening large volumes of data.

2. Train Staff

Educate employees on identifying and managing compliance risks associated with sanctions. Training should focus on recognizing red flags and using sanction screening tools effectively.

3. Maintain Audit Trails:

Keep detailed records of screening activities, including dates, results, and actions taken. This documentation demonstrates due diligence during audits or investigations, which is crucial for HIPAA and insurance compliance.

By leveraging services such as those provided by Compliance Resource Center, telehealth programs can efficiently integrate sanction screening into their compliance workflows. With proprietary software to automate screening, using up-to-date data from all relevant sanction lists, we make it time-efficient and cost-effective to regularly audit your vendors and providers to maintain compliance. Better still, our flexible training services offer both in-person and digital sessions to equip your employees to manage a safe and compliant telehealth program.

Want to explore how they could help your organization implement a safe and secure telehealth program?

Book a Consultation