OIG Background Checks: What to Know and How to Prepare

A single employee or vendor on exclusion lists can cost your healthcare organization six figures and/or harm your reputation – but there is a reliable process to avoid this fate. OIG background checks are a vital part of any healthcare compliance program, ensuring you never hire or partner with an excluded individual or entity and remain fully OIG compliant.

This article explains what that means in practice and provides a proven framework to help you implement and scale OIG background check best practices. But first, let's establish why compliance leaders should care about this topic.

OIG Background Checks: Understanding the Basics

What is an OIG Background Check?

An **OIG background check** is a form of screening that assesses whether a specific individual or entity has been excluded from participating in Medicare, Medicaid, and other federal healthcare programs. These checks ensure compliance with federal regulations and protect patients from unqualified providers.

But how exactly are these background checks undertaken?

The OIG Exclusion List

The U.S. Department of Health and Human Services (HHS) is responsible for maintaining a database of excluded individuals and entities known as the **List of Excluded Individuals and Entities (LEIE)**. This currently includes more than 74,000 individuals and 3,200 organizations barred from participating in federally funded healthcare programs due to violations such as:

- **Mandatory exclusions** (e.g., Medicare fraud, patient abuse, felony drug convictions)
- **Permissive exclusions** (e.g., misdemeanor fraud, professional license revocation, defaulting on health-related loans)

OIG background checks search the LEIE to determine whether an individual or entity is listed.

Who Should Be Screened?

Healthcare organizations must screen:

- **Employees**: All clinical staff (e.g., doctors, nurses, therapists) and administrative personnel involved in patient care or billing
- **Contractors and Vendors**: Third-party service providers, including medical equipment suppliers, IT service providers, consultants and temporary staff
- **Volunteers:** Individuals who may have access to patient information or participate in patient care activities

Any failure to do so will lead to a range of problems – including steep fines and reputational harm.

Importance of Conducting OIG Background Checks

There are two primary reasons organizations should prioritize OIG background checks:

1. Legal and Regulatory Compliance

The OIG exclusion list is not advisory; it is illegal to work with excluded individuals or entities - and non-compliance can lead to a range of penalties:

- **Financial Costs:** Employing an excluded individual leads to eye-watering fines. Recent settlements have reached six figures, with one provider fined over $150,000 for employing a nurse they were unaware was featured on the OIG exclusions list. Crucially, the OIG can argue that your organization *should* have known the individual or entity was excluded – and factor that into the total financial claim.
- **Insurance Losses:** Care delivered by excluded individuals will not be reimbursed – potentially leading to steep losses. Not only is the treatment not repaid by Medicare or Medicaid, but allowing excluded individuals to administer care is illegal and has led to $27 million in fines against numerous providers.
- **Reputational Damage:** The OIG regularly publishes reports of organizations penalized for non-compliance, functioning similarly to HIPAA's "Wall of Shame." This is publicly available and may negatively impact recruitment and patient acquisition or retention.

2. Protecting Organizational Integrity

Exclusions are often the result of low-quality service, Medicare fraud, or even patient neglect. Screening individuals and vendors is, therefore, a vital safeguard against malpractice – and a key priority to protect patients from harm.

How to Conduct OIG Background Checks

Most OIG background checks are undertaken manually using the OIG's database. The database is publicly available via an online search portal, and a basic background check is as simple as searching the individual or organization's name.

Organizations can:

- Search for individuals/entities **by name or National Provider Identifier (NPI)**
- Download the full **monthly updated list** for bulk searches
- Use name variations to **avoid false negatives**

If an individual is flagged on the LEIE, compliance officers should:

1. **Verify Identity:** Avoid false positives by checking name variations and associated aliases, along with the individual's NPI and Social Security Number (SSN).
2. **Review Employment History:** Assess the employment record to determine whether they directly or indirectly participate in federally funded programs, including subcontracted or vendor-related work.
3. **Consult Legal:** Ensure appropriate steps are taken in accordance with federal and state regulations, documenting the decision-making process for future audits.
4. **Resolve the Issue:** This might mean immediate termination, temporary suspension, notification to relevant authorities, and guidance on how the individual may apply for reinstatement if applicable.

In theory, this process is relatively straightforward and protects your organization from the prospect of non-compliance. But there are several factors that make OIG background checks more complicated.

Challenges in OIG Background Checks

Healthcare organizations of all sizes face three pervasive issues when running OIG background checks:

1. Data Accuracy and Updates

The OIG exclusion lists are reliant on state reporting, and their frequency and accuracy are highly variable. While States are required to report new exclusions within 30 days, the actual average time is 173 days. This leaves **nearly 6 months** during which organizations might onboard an employee or vendor that will subsequently prove to be excluded.

2. Managing False Positives

Given the number of individuals and entities included in exclusion lists, it is not uncommon for false positives to emerge. An employee may share their name with an excluded individual, and a simple manual search will make them *appear* to be excluded themselves.

Cross-referencing using additional information to confirm the individual's true identity is therefore essential. But this creates extra effort for compliance teams and can be highly time-consuming – especially when you consider how much effort screening programs already entail.

3. Scale of Screening Requirements

While OIG background checks are not a heavy burden in themselves, they must be taken into account in the proper context. Healthcare compliance teams are tasked with screening every individual and vendor across numerous lists – from the System for Award Management (SAM) list to TRICARE, OFAC, and FDA exclusions.

The total workload is substantial, and many compliance teams are already under-resourced. Add to this the fact that many States maintain their own exclusion lists and federal contract recipients must be screened in addition to OIG background checks – and you start to see how screening can become inconsistent or simply fall through the cracks.

Best Practices to Maintain OIG Compliance

The challenges above are extremely common, but after decades at the forefront of healthcare compliance, we have established a clear process to overcome them and make OIG background screening a standard operating process (SOP) at organizations of all sizes:

1. Frequent Screening

The first step is to ensure you are meeting the correct frequency with OIG background checks. Best practices recommend screening during:

- **Employee Hiring:** This ensures that no new employees or contractors are listed in the OIG exclusion database before being brought on board.
- **Vendor/Supplier Due Diligence**: All third-party service providers must be vetted before agreements are finalized to mitigate compliance risks.
- **Post-acquisition/Merger**: When acquiring a healthcare entity, screening all inherited employees and contractors is critical to avoid financial and reputational risks.
- **Monthly Re-Screening**: Since the LEIE is updated frequently, organizations must conduct recurring checks to ensure continued compliance.

2. Record-Keeping Practices

Next, we must ensure that you maintain comprehensive documentation of all screenings to prove due diligence and combat potential claims of negligence. Organizations must:

- **Store Search Results**: Retaining copies of searches ensures a verifiable history of due diligence in compliance efforts.
- **Implement Internal Policies** for managing identified exclusions: Defining clear guidelines for what actions to take when an excluded individual is discovered ensures consistency and mitigates liability.
- **Ensure Reporting Compliance**: Reporting protocols should align with federal and state regulations to demonstrate a proactive approach to compliance.
- **Develop an Audit-Ready Process**: Implementing an internal audit process for verifying and documenting screenings will help organizations defend against potential OIG investigations.

3. Employee Training

OIG background checks require skilled professionals who understand the process in detail. This often requires dedicated compliance training to ensure you have adequate screening processes in place – and can run them properly.

For example, your team must be aware of the prospect of false positives and follow the steps outlined above to avoid them. This should become second nature; no action should *ever* be taken without thorough verification of the individual or vendor's identity.

4. Leverage Technology

The final step is scaling your program – and this may be the most challenging of them all. As discussed above, the sheer volume of manual effort involved in a complete screening program outstrips most organizations' compliance resources, which is why many are opting to use advanced software to automate the process.

Streamline Sanction Screening with Compliance Resource Center

Compliance Resource Center offers sanction screening software that enables compliance teams to check all lists and exclusions with ease. Based on the most up-to-date data available, the software can be used for either single-name or batch-processing to assess all employees and vendors with confidence – and reduce the burden on your resources.

Want to explore how it could help you stay OIG compliant?

Get Your Consultation