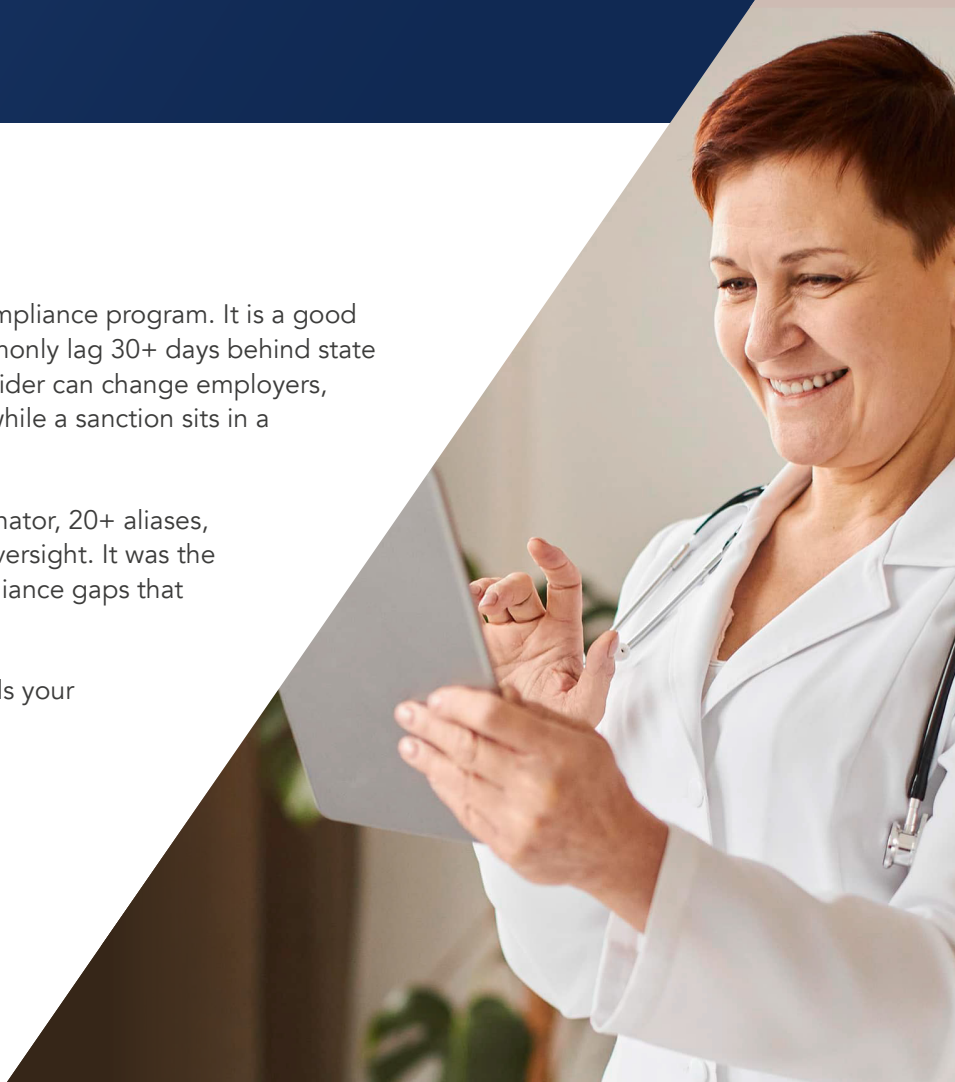
Verisys®

Closing the Five Critical Gaps in Healthcare Screening

UBS x VERISYS

The question isn't whether your organization screens at hire, as every organization should. The question is: **what happens between or after initial screening?**



WHY THIS CHECKLIST EXISTS

A clean background screening at hire is not a compliance program. It is a good starting point. Federal exclusion databases commonly lag 30+ days behind state board disciplinary actions. In that window, a provider can change employers, cross state lines, and continue treating patients while a sanction sits in a system that hasn't caught up.

The Shannon Nicole Womack case, one impersonator, 20+ aliases, six states, undetected, wasn't the result of one oversight. It was the accumulated space between five common compliance gaps that exist in most healthcare organizations today.

This checklist maps those five gaps to the controls your program should have in place.

verisys.com

universalbackgroundscreening.com

The Five Gaps and What to Check

Gap 1: Name Matching

THE RISK:

Bad actors exploit systems that only screen the name provided on an application. Using aliases, nicknames, maiden names, or slight name variations, they can bypass name-based watchlists entirely.

WHAT TO CHECK:

- Are candidates screened using SSN + date of birth in combination with their name?
- Are alias flags tied back to a primary identifier so variants can't slip through independently?
- Are you using fuzzy boolean logic when it comes to name matching or checking aliases?

Gap 2: Single Source Exclusion Screening

THE RISK:

Relying on a single exclusion database, even the OIG/GSA, leaves organizations out of compliance. State-level disciplinary actions are often the earliest signal of a problem, and they don't appear in federal systems for weeks or months.

WHAT TO CHECK:

- How many sources do you have access to check?
- Does your monitoring solution draw from multiple databases?
- What frequency do the sources update that you are checking?
- Are you using a solution with multiple primary sources at the state, federal, and board levels, not just OIG, SAM.gov, and your state Medicaid exclusion list?
- Have you confirmed with your compliance team that your current vendor covers all required sources for your accrediting bodies (NCQA, URAC, The Joint Commission, CMS)?

Gap 3: Cross-State Reporting

THE RISK:

A provider disciplined in one state may hold active licenses in two or three others. State boards do not automatically share information with each other. Without multijurisdictional monitoring, that information never reaches the employer holding the credential.

WHAT TO CHECK:

- Does your monitoring program cover all 56 U.S. jurisdictions, including territories?
- Are providers screened in every state where they hold or have held a license, not just the state where they currently work?
- Is your system actively monitoring across all jurisdictions in real time, not just at the point of hire?

Gap 4: Federal Reporting Lag

THE RISK:

The risk Federal databases reflect disciplinary actions 30+ days after state licensing boards publish them. That month is not a rounding error; it is enough time for a provider to change employers or relocate while a sanction sits undetected.

WHAT TO CHECK:

- Are you monitoring primary sources directly, not just waiting for federal databases to update?
- Does your solution include "leading indicator" sources such as state board meeting minutes and agency press releases?
- Can your program surface a risk signal days or weeks before it appears in federal systems?
- Are alerts delivered in real time (via API, SFTP, or portal), not batched in a weekly or monthly report?

Gap 5: Continuous Monitoring

THE RISK:

Most organizations conduct a thorough check at hire, then sometimes rescreen on a cycle. A license can lapse, sanctions can be issued, and malpractice can be recorded in the month between scheduled reviews, without anyone being aware until it becomes a problem.

WHAT TO CHECK:

- Has your organization moved from periodic re-screening to perpetual credentialing, an always-current view of every provider's status as well as post-hire criminal monitoring?
- Is your monitoring continuous, or does it rely on scheduled annual or semi-annual rechecks?
- Do you have documented workflows for receiving, reviewing, and escalating alerts?
- Are post-hire changes in license status, exclusions, or sanctions automatically surfaced to the credentialing team or cross-departments within your organization?

Program Readiness: The Bigger Picture

Beyond the five gaps, a defensible compliance program also requires:

Accreditation Alignment

- Your program follows FCRA
- You can produce a primary source verification audit trail on demand for Joint Commission surveyors
- CMS participation requirements are addressed, including exclusion monitoring for all provider types

Identity and Onboarding Foundation

- SSA/DMF Search or CBSV
- Identity validation at hire includes document verification and SSN trace — not just name lookup
- FCRA-compliant processes are in place for adverse action and dispute resolution
- Multi-jurisdictional criminal history research covers the candidate's full residential history

Operational Readiness

- Your compliance, HR, and credentialing teams have a shared escalation protocol for monitoring alerts
- Vendor turnaround timelines, reporting formats, and dispute processes are documented and consistent
- You are not relying on multiple vendors whose data doesn't align when an auditor asks for a unified record



The Cost of Non-Compliance

The annual cost of comprehensive exclusion monitoring is a fraction of the exposure a single missed sanction or record can create.

A single CMA exclusion violation can trigger:

- Repayment demands on previously billed claims
- Civil monetary penalties
- In severe cases, program exclusion

The DOJ secured $1.7 billion from healthcare False Claims settlements in 2024 alone. A good question your CFO or Compliance team should be answering is not 'what does monitoring cost?' It is 'what does a missed sanction cost?'

Background screening is a standard part of hiring and risk management. Recent data shows that approximately 94–95% of U.S. employers conduct background checks as part of their hiring process.

In the U.S., roughly **one in three adults has a criminal record**, increasing the likelihood that relevant history exists beyond what is self-reported.

In regulated environments like healthcare, that exposure carries real consequences. Civil monetary penalties for employing excluded individuals can reach up to $10,000 per item or service billed, and negligent hiring claims continue to result in substantial financial settlements when issues are missed or discovered too late.

The Verisys + UBS Solution

Universal Background Screening establishes a compliance foundation at hire through multi-jurisdictional background screening, identity verification, and FCRA-compliant processes. Recognized as the #1 enterprise screening firm by HRO Today for 14 consecutive years.

Verisys powers the continuous compliance layer with FACIS® 3, the most comprehensive healthcare exclusion and disciplinary monitoring database available, drawing from 5,600+ primary sources and 900+ leading indicator sources, and covering all 56 U.S. jurisdictions across 800+ provider taxonomies. Verified accuracy: 99.97%. Currently monitoring more than 15 million individuals and entities.

Together: a seamless compliance lifecycle from onboarding through perpetual credentialing and monitoring.



verisys.com

universalbackgroundscreening.com