Background Checks: An Essential Risk Management Tool

By Stefan Keller

Executive Summary

The safety of patients and their information, and similarly staff and their information, is an obligation of healthcare management. Hospitals are a target. Today, protection is becoming a unique challenge which requires active efforts to ensure adequate safeguard levels. Patients, staff and information are at risk—as is your organization's reputation. While there are regulatory requirements covering some aspects of these issues, providers are well-served to consider the value of performing background checks on all proposed new hires and establishing a program of regular inquiry regarding possible sanctions and criminal behavior of their staff. Establishing such a program limits employer liability by demonstrating that reasonable care has been exercised.

Introduction

A nursing assistant previously arrested for rape and fired from another job for sexually harassing a female patient rapes a paralyzed stroke victim in her hospital room. An emergency room clerk steals the names and Social Security numbers of dying patients and opens credit cards in deceased patients' names. A licensed practical nurse who appears on the General Services Administration's (GSA) Excluded Parties List System (EPLS) alters her name to avoid detection; the hospital that hires her is later fined.

These examples illustrate the myriad—and overlapping—pressures hospitals face in three critical risk areas: ensuring the safety of patients and staff, protecting records and data from unauthorized use or release, and ensuring regulatory compliance.

While each of these areas poses its own unique set of challenges, they have one preventative weapon in common: background checks. Psychologists and criminologists agree that the strongest predictor of future criminal behavior is past criminal and delinquent behavior. Background screening of prospective and existing employees, contractors, and temporary workers reveals past behavior and gives hospitals a tool to manage risk.

Protecting Patient and Staff Safety

Pre-hire screening of prospective employees helps ensure that an individual is properly qualified for a specific position and can reveal past acts or behavior patterns that make someone unsuitable for employment in a healthcare setting. Likewise, periodic screening of existing employees is important to ensure legal and regulatory compliance and to uncover negative behaviors that occur post-hire.

The safety of patients and staff is one of the primary drivers of healthcare-worker background checks, particularly in light of some highly publicized cases. The most famous case is that of Charles Cullen, a nurse nicknamed the 'Angel of Death'. Over a 16-year period, Cullen used lethal drug injections to kill up to 40 patients at multiple Pennsylvania and New Jersey hospitals.

Cullen's case revealed a troubled work history. He bounced from hospital to hospital, volunteering for overnight shifts where he often went unsupervised, and resigning when he aroused suspicion. In cases where he was fired, many of the hospitals gave vague reasons for his dismissal, such as poor performance.

As a direct result of the Cullen case, New Jersey law now requires healthcare entities, upon inquiry, to provide the following information about current or formerly employed healthcare professionals: (1) job performance as it relates to patient care based on job performance evaluations; (2) eligibility for re-employment at the healthcare entity; (3) reason for separation for a formerly employed healthcare professional; and (4) copies of any notifications and supporting documentation sent to the New Jersey Division of Consumer Affairs (DCA), the medical practitioner review panel, or a DCA professional or occupational licensing board within seven years of the inquiry date.

> The strongest predictor of future criminal behavior is past criminal and delinquent behavior.

Many other states have employer reference immunity laws in place to protect employers from being sued for providing a negative employment reference. Most of these laws require healthcare entities to disclose *truthfully* to a prospective employer whether

Online assistance:

US Equal Employment Opportunity Commission	www.EEOC.gov/
US General Services Administration	www.epls.gov/
US Dept. of Health and Human Services, Office of Inspector General	www.oig.hhs.gov/
Dept. of Homeland Security	www.uscis.gov/e-verify
US Social Security Administration	www.ssa.gov/onlineservices/
US Treasury	www.ustreas.gov/offices/enforcement/ofac/sdn/

an employee was reported to a state licensing or review board. An employer acting in good faith and without malice is generally granted immunity from civil liability.

The Cullen case spotlights the need to conduct thorough background checks that include, at a minimum, Social Security number verification/validation, a criminal records check, education and employment verification, and reference checks. While checking items like criminal history may seem like common sense, checks such as education and professional license verification can reveal inconsistencies and patterns of dishonesty that may indicate deeper problems with an applicant's background.

Should a bad actor emerge clean from a background check, or commit bad acts post-hire, background checks can also help to protect hospitals against negligent hiring lawsuits. In those cases, the employer is liable for damage caused by an employee when it should have known of the employee's propensity to commit injury. If a background check is performed, the hospital may be able to mitigate risk by demonstrating it has a systematic process designed to identify and prevent the hiring of individuals with questionable backgrounds.

Protection of Confidential Information

Hospitals are a prime target for identity theft—America's fastest-growing crime, with as many as nine million victims annually. Confidential information, like Social Security numbers, dates of birth, billing/payment information and medical records, is available in many locations in the hospital, including billing, admissions, medical records, patient rooms and charts.

Hospital Human Resources (HR) departments, in particular, are vulnerable to identity thieves because they maintain exactly the type of records fraudsters seek. Plus, HR is subject to federal regulations governing employer disposal of applicant and employee records, which also creates a compliance concern. Employer liability centers on the legal standard of 'reasonable care'. For example, information stolen from an open file cabinet is viewed differently than information stolen from a locked file cabinet, since the locked cabinet demonstrates that the employer made a reasonable effort to protect the information.

While hospitals are familiar with the need to guard protected health information (PHI), it's also critical to protect personal identifying information (PII). PII is information which can be used to distinguish or trace an individual's identity, such as their name, SSN, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as a date and place of birth and mother's maiden name.

Identity theft occurs when someone uses an individual's PII without permission to commit fraud or other crimes. PII is also used in medical identity theft, which occurs when someone uses a person's name and/or other parts of their identity—such as insurance information—to obtain or make false claims for medical services or goods. Identity theft poses a risk primarily to the individual whose identity is stolen, but medical identity theft poses a risk to both the patient, who faces the risk of improper treatment if the identity thief's medical history is mixed with theirs, and the hospital, which faces the risk of liability for improper treatment if a chart contains incorrect information.

In hospitals, identity theft can take a number of forms. Common techniques include dumpster diving, in which personal information is stolen from discarded papers; changing the victim's address to divert billing statements; and simply stealing wallets, personnel or billing records or other items containing personal information. Additionally, identity theft can occur through data breaches, which involve lost or stolen digital media and mistaken Web postings.

Background checks can identify previous financial crimes, including identity theft. While many organizations only conduct credit checks on applicants for positions involving access to cash or financial information, many other positions present the opportunity to commit identity theft. The emergency room clerk who stole deceased patients' identities is an example, as the position gave her access to the patient personal information necessary to commit identity theft.

To combat identity theft, hospital HR and medical record departments can protect confidential information and patient privacy by locking up patient and employee personal information and limiting access to only those who need it to perform their jobs. HR departments can perform background checks on employees, volunteers and temporary workers. Additionally, vendors should provide hospitals with evidence that they screen their employees and follow proper data handling procedures.

Regulatory Compliance

Because healthcare is highly regulated, hospitals must comply with a wide variety of federal and state-level regulations, as well as those promulgated by healthcare organizations, such as the Joint Commission.

Sanctions screening, including LEIE and EPLS checks, is one of the primary background check tools used to achieve regulatory compliance. Under federal law, hospitals are not permitted to hire any individual or contract with any business appearing on either of two lists: the

U.S. Department of Health and Human Services Office of Inspector General (OIG) List of Excluded Individuals/Entities (LEIE), which lists individuals barred from participating in federally funded healthcare programs based on convictions for program-related fraud and patient abuse, licensing board actions and default on Health Education Assistance Loans; and the General Services Administration's Excluded Parties List System (EPLS), which lists individuals and firms excluded by federal government agencies from receiving federal contracts or subcontracts.

> *The safety of patients and staff is one of the primary drivers of healthcare-worker background checks.*

Hospitals that hire or contract with an individual or business appearing on the OIG or GSA lists risk sanctions including fines and possibly the loss of Medicare/Medicaid funding. As a result, many institutions conduct OIG/GSA checks on prospective employees prior to extending the offer to hire and on existing staff on a monthly or quarterly basis.

It is also critical to check national accrediting organizations and state licensing and regulatory bodies to ensure that any professional licenses reported by an applicant are valid and that no sanctions or disciplinary action has been taken against the individual.

For example, a Georgia hospital checked a temporary employee and discovered her Ohio nursing license was voluntarily suspended due to allegations of patient abuse. The individual had obtained a Georgia nursing license before the Ohio Board of Nursing posted the suspension information. Because states don't always share information, sanctioned individuals can—and often may—simply move out of state to avoid detection.

Additionally, screening helps hospitals to comply with the Joint Commission's Standard HR.1.20, which includes a provision that hospitals must have a process to ensure that an individual's qualifications are consistent with his/her job responsibilities. A proposed clarification listed in the Joint Commission's 2009 Comprehensive Accreditation Manual for Hospitals states, "The hospital verifies and documents that the applicant has the education and experience required by the job responsibilities".

Adding the word 'documents' clarifies that hospitals should create a record of the verification steps taken. For example, to verify an applicant's nursing license, it is acceptable to call the state licensing board and confirm the applicant's licensure validity and status. However, under the standard, that phone conversation must be documented. That requires the hospital HR representative to write down and file when the call was placed, to whom they spoke, the applicant's license number and expiration date. If the check is conducted online, a time and date-stamped printout of the information should also be retained.

Background Checks

A typical hospital employee background check includes the following components:

Social Security Number Verification/Validation

This check confirms a person's identity using their Social Security Number, ensuring the number is valid and that it belongs to that individual. Social Security Number verification and validation are conducted using a 'trace report', which pulls the non-financial header portion of an applicant's credit report.

Similarly, the trace report is used to confirm an applicant's address history; an applicant who is hiding a past crime or sanction may not disclose previous addresses on the employment application. Address history also helps determine where criminal searches are conducted, as it shows an applicant's current and past counties of residence.

Social Security Number verification is also achieved through E-Verify, a federal database that compares the information provided on the I-9 form to Department of Homeland Security and Social Security Administration databases to confirm employment eligibility. E-Verify use is voluntary at the federal level, but a number of states require some or all employers to participate. Regulations are also pending to require E-Verify use by certain federal contractors.

Criminal Records

Criminal record searches can be performed at numerous levels: national criminal databases and federal, statewide and county criminal records.

Private national criminal databases can be an excellent background check tool, but cannot be relied upon solely. Information contained in national databases is often outdated and typically lacks identifiers that allow the user to confirm that records belong to the subject. It is best utilized as a double-check for county and statewide criminal record searches.

The most effective criminal record searches are court searches—either electronic access to court-maintained databases or physical searches of court records. Federal searches encompass records found in 100 federal district courts nationwide. Statewide searches are either state police-based or centralized court-based. While offering broader coverage, statewide criminal records searches are often less accurate or are not updated frequently because they rely on information to be reported up from the county level. As such, a county or municipal court search offers the most accurate and up-to-date source of criminal records information. Specific state regulations may also mandate fingerprinting or a certain type of criminal search based on the position and/or contact with vulnerable populations.

Registry Searches

Given the access that healthcare workers have to vulnerable populations—children, the elderly, and the disabled—checking both sex offender and abuse registries is of paramount importance. Sex offender registries are available in most states and nationally through national criminal databases. Many states also offer child abuse, elder abuse, and nurse-aide misconduct registries.

Education, Employment and License Verification

Education history verification involves contacting educational institutions to confirm degrees obtained and areas of study. Ensuring an individual's educational credentials are valid helps to ensure that the applicant is sufficiently qualified under the Joint Commission HR.1.20 Standard.

In the case of employment history, previous employers are contacted to confirm dates of employment and identify any gaps, as well as to confirm position/title, job responsibilities and performance, reason for leaving and eligibility for rehire. Reference checks should also be conducted as part of the employment history verification process to determine information about an applicant's character.

Professional license/designation verification is conducted in the same way—the issuing authority is contacted to determine a license's validity and current status. A professional license/designation search can also include searching OIG and GSA excluded parties lists and other sanctions lists.

Credit Check

A credit report from one of the three credit bureaus shows an applicant's financial history, including bankruptcies and liens. Some hospitals may choose to run a credit report only on those in positions with access to financial information or cash, but it can help identify any applicant's potential to commit financial crimes or identity theft.

What to Do With Background Check Results

Once a hospital receives the results of a background check, there is often uncertainty about what to do with the information.

First, while you are building a background check program, it is important to determine your organization's hiring criteria, and what is acceptable and unacceptable according to organizational policy, federal and state law. That process should include determining risk assessment issues specific to your hospital and weighing the risk factors involved in making a hiring decision.

In terms of criminal records, the Equal Employment Opportunity Commission (EEOC) prohibits organizations from issuing a blanket 'no convictions' hiring policy. Instead, the employer must provide the applicant with an opportunity to explain the circumstances of an arrest and make a reasonable effort to determine whether the applicant's explanation is credible before refusing to hire him or her. As such, in deciding whether or not to hire someone with a criminal conviction, it is important to assess the nature and gravity of the offense; the time elapsed since the conviction or sentence completion; and the nature of the position. When it comes to arrest records, the employer must consider the same elements as convictions, but also evaluate the likelihood that the applicant actually committed the conduct alleged in the arrest record. Additionally, state laws must be considered before using arrests and/or convictions in making hiring decision, as many states limit the reporting of arrest records and non-convictions.

Once organizational policy is established and all legal aspects are taken into consideration, evaluating results is a matter of determining what does and does not add up. Look for red flags in the application or on the background check results, such as unclear or incomplete answers, skipped questions on the application and negative information returned on the background investigation. When you receive results, ask the applicant about anything that doesn't make sense, such as an inconsistent Social Security number or employment history.

Summary

Establishing a background check program can reveal potential problems in an applicant or employee's background to allow hospitals to filter out bad actors to better protect patient and staff safety, confidential information and regulatory compliance efforts.

Stefan Keller is president of Certiphi Screening, Inc., an applicant screening firm that serves the healthcare community exclusively and is the only company whose applicant screening services are endorsed by the American Hospital Association. He can be reached at skeller@certiphi.com.

Reprinted with permission from New Perspectives, Journal of the Association of Healthcare Internal Auditors, Inc. Volume 28 Number 2.