

# Complete Healthcare Compliance Manual 2024 Auditing

---

By Mary M. Menard,<sup>[1]</sup> RN, MPH, CHC, CHPC

Auditing is a discrete, planned event in which a focused and structured process is designed to independently evaluate a distinct area of the organization or practice. Audits help to ensure that the practice or organization remains vigilant in its compliance efforts. There are many types of audits, including internal and external audits and prospective and retrospective audits.

## Internal Audits

These audits are formal reviews of compliance with a particular set of standards (for example, policies, procedures, laws, and regulations) used as base measures. Internal audits are performed by individuals who are independent of the process being audited. In other words, by individuals who do not actually work in or manage the area being studied. The idea is to concentrate attention on matters that have been causing the organization or practice problems with compliance, as indicated by the results of ongoing monitoring activity, risk assessment, or other reports, or areas that may cause the organization compliance concerns, such as issues identified by the Centers for Medicare & Medicaid Services (CMS), areas of heightened enforcement concerns as reflected in the Office of Inspector General (OIG) Work Plans, special fraud alerts, audits, CIAs, and other law enforcement initiatives.

Internal audits should focus on one aspect of the responsibilities of a department or section. If the policy is multifaceted, then detailed criteria for the audit should be itemized. It is best to keep each audit directed so that both the review and the results are manageable. An audit that attempts to accomplish too much at one time has an increased opportunity for failure. Consider conducting several smaller audits rather than one large investigation unless you have the time and workforce to complete the bigger scope.<sup>[2]</sup>

Audits may be prospective or retrospective. Prospective audits examine a system in action, as it is happening, whereas a retrospective audit looks at work that has already been done. An example of a prospective audit is a prepayment claim review in which claims are reviewed before they are submitted for payment, therefore allowing for correction if a problem exists. On the other hand, claims that have already been submitted for payment and are then selected for audit are being reviewed retrospectively (or after the fact). Retrospective audits are often used because the data is more easily obtained for sampling and the sample is usually more complete. Retrospective audits are also used to establish a baseline or reference point of the provider's current policies and practices.

Based on the findings of an internal audit, the organization or practice may implement a corrective action plan that may alter work processes and current policies, establish measurable improvement goals, result in repayment of an overpayment, or conclude that there is not enough evidence to warrant significant changes. Internal audits provide a mechanism for preventing, or at least mitigating, problems before they create significant legal risk. Audits are an important element of an effective compliance program.

Audit findings must be documented and reported to senior management, the compliance or audit committee, and the governing body. The audit report should include findings of noncompliance and/or suspicions of

misconduct and an action plan to address and resolve each potential problem, including planned follow-up actions.

If the audit identifies reportable violations, the provider should plan for voluntary disclosure to the applicable government agency. Before acting, however, the provider should contact its attorney for guidance.

## External Audits

These audits are performed by someone outside of the organization or practice, such as an independent auditor, a government contractor, the OIG, a government program, or a commercial payer. External audits will be discussed later in this article.

## Defining the Audit

Auditing is not a one-size-fits-all process. Auditing topics, scope, and methodology will vary by provider type, size, risk priority areas, and available resources. The OIG's Compliance Program Guidance for various healthcare providers and suppliers was meant to encourage the development and use of internal controls to monitor adherence to applicable statutes, regulations, and program requirements.<sup>[3]</sup> These guidance documents are a must-read for anyone in healthcare compliance and audit. Provider-specific risk areas are identified and discussed, as are methodology and sample selection, best practices, and recommendations.

An important element in all compliance programs is the risk assessment (discussed in chapter 3). A thorough risk assessment should identify all known and suspected risk areas applicable to the provider, assess the probability and impact to the provider if the risk were to occur, and prioritize risks to establish a most-to-least-critical importance ranking. Those risks identified as having a high probability and high impact should be assessed for ongoing monitoring or auditing.

### Common High-Risk Areas for Providers and Suppliers

- Coding
- Billing
- Documentation
- Medical necessity
- Financial relationships with physicians (compliance with Stark Law)
- Anti-kickback schemes
- HIPAA privacy and security
- Cybersecurity

Telehealth is also a high-risk area, particularly as a result of the COVID-19 public health emergency when CMS implemented a number of waivers and flexibilities that allowed Medicare beneficiaries to access a wider range of telehealth services without having to travel to a healthcare facility. This resulted in unprecedented increases in

telehealth and the possibility for fraud in telemedicine. CMS and other payers will need to monitor program integrity implications and address the potential for fraud and abuse in telemedicine. Hence, there will probably be an increase in external audits of services provided by telemedicine.

Other areas to monitor closely for potential high risk include government actions—or headline-making settlements—as they are a bellwether of future audits, CMS contractor audits, and the OIG Work Plan. The OIG Work Plan lists various audits and evaluations that are underway or planned during the fiscal year and beyond.<sup>[4]</sup> The Work Plan is dynamic, and the public-facing Work Plan is updated monthly.

Monitoring activity, findings in an audit, and reports made to the compliance officer may also result in the need for a discrete audit, which may be a full audit or a smaller, focused or probe audit. The OIG states in its guidance documents that one of the most important components of a successful audit protocol is an appropriate response when the practice or facility identifies a problem. This action should be taken as soon as possible after the date the problem is identified, noting that the specific actions should depend on the circumstance of the situations. So an audit plan should remain flexible to accommodate changing risks and audit needs.

This document is only available to subscribers. Please log in or purchase access.

[Purchase](#) [Login](#)