Trust but Verify: Safeguards in Contracting for Outsourced Coding Services

Save to myBoK

By Ajit Sett, MBA, ACA; George T. Hickman, LCHIME, LFHIMSS, CPHIMS, CHCIO; and Karen Karban, RHIT, CCS

Coding is an essential task in a care delivery organization (CDO) and represents the convergence of certain clinical and financial processes. It is the culmination of the documentation and codification of provided patient care services and the identification of associated charges and claims. Revenue is truly dependent on the completion and integrity of the coding process, and clinicians need assurance that codes are consistently and accurately representing the nature of the patient health condition and the service rendered to improve or maintain those health conditions. Further, coding efficacy must stand up to payer, compliance, and audit requirements.

There is a well-documented shortage of coders in the United States. Productivity concerns associated with ICD-10-CM/PCS implementation will only cause the situation to worsen. Historically, HIM directors have addressed overflow coding needs by engaging local companies to provide staffing under the guise of an independent contractor arrangement for after-hours support. These "moonlighters" are increasingly needed by CDOs.

To mitigate coder shortage risks, many CDOs are exploring options to partially or fully outsource coding services. Deployment of additional on-site coding resources for an extended period of time can be costly, thereby necessitating a move to remote coding services. Despite the move to remote coding services, some US-based organizations cannot keep up with the demand for resources. This has led some CDOs to turn to outsourced, remote, and offshore coding services.

Discovery Questions and Contract Considerations for Outsource Coding Vendors

Vendor Discovery Questions	Due Diligence and Contract Considerations
Demonstration of adherence to HIPAA "minimum necessary" use and disclosure guidance Intent to store PHI for any purpose beyond initial coding effort	• Require the vendor to complete the coding task directly in the electronic health record (EHR), financial or HIM system, and cloud-hosted portals. • Require the vendor to certify that they will not store any part of the patient record in any form (PHI, de-identified health information, limited data set) or use information for any purpose other than the scope of the engagement. • Ensure the vendor's storage and/or use of all or any part of the patient record in any form does not violate the intent of the federal laws (HIPAA), state laws, the HITECH-HIPAA Omnibus Final Rule's use and disclosure requirements, and the entities' own organizational standards relative to their Notice of Privacy Practices. Ensure the current business associate agreements are compliant with Omnibus Rule updates. By law, CDOs must rely on professional ethics and best judgment in deciding which permissive uses and disclosures of PHI to make. CDOs' risks are minimized if the vendor codes within their EHR/HIM/encoder systems and does not store or use any part of the patient record, in any form (i.e., PHI, de-identified health information, limited data set). HIM systems include cloud-hosted portals, where the patient record is dropped for processing and then returned to the client's systems via a HL7 feed.

	There is no need for a vendor to store patient information in any form. Vendors can simply access the record via a VPN; the patient record resides on the CDO's system and should remain there. Coding audits, re-coding to address claim rejections/denials, RAC defense, etc. can be supported by re-accessing the EHR and other information systems and/or scanned images.
Compliance with the addressable and required HIPAA Security Rule standards and a CDO's own security best practices	CDOs must assess their security risks, which is one of the foundations of HIPAA Security Rule compliance. The following review areas, which pertain to outsourced coding services, are in addition to the CDO's standard security checklists. • Information Security Policies and Procedures: ◦ Ensure the vendor has established a set of policies and standards that steer the behavior of their remote coding resources toward secure practices, including strong password management, password change and access timeouts, protected health information (PHI) storage/use/destruction, data encryption, PHI exchange procedures, privacy filters, etc. These policies and standards are especially important when remote coding resources are not working from secure production facilities or are working from their own home. ◦ Ensure the vendor can demonstrate policies in practice. • Endpoint/Mobile Security: ◦ Ensure the vendor has an adequate mobile security policy. ◦ Ensure PHI can be accessed from a device only from a workstation in a secure production facility; ensure all devices have licensed copies of software and receive mandatory updates for virus, spyware, malware, and related protection and software updates; print screen functions are de-activated; and all data storage options are disabled. ◦ Ensure the vendor issues fully secure devices to remote coding resources which only allow access to a CDO's EHR, HIM, and encoding systems for remote coding purposes. ◦ Ensure the vendor's employees sign confidentiality statements that cover privacy expectations, workstation security, and safety as well as a remote workforce agreement. • Data Network Security: ◦ Ensure the vendor's servers, cloud, and networks are protected when connecting remotely via an electronic device or computer. Encourage remote connection via a VPN that requires two-factor authentication to provide more assurance against the risk of unauthorized access to patient data. ◦ Ensure the vendor leverages intrusion detection services and security services like use of firewalls, and is current with antivirus software and patch management to further secure endpoints. ◦ Ensure the vendor's routers, switches, and other devices meet HIPAA compliancy requirements to protect ePHI found on networks. ◦ Ensure the vendor meets required standards by establishing policies limiting software program access to only those with authorized access. ◦ Ensure the vendor maintains data at rest (i.e., on stored media such as hard drives or USBs) and data in motion as transmitted over wireless,

	wired networks, or the Internet are encrypted to the required current HIPAA NIST standards or better.
	
	• Breach Response:
	  ◦ Review the vendor's contract and business associate agreement for their breach notification roles and responsibilities, and make sure that the breach notification policies are fully aligned so that a CDO can accurately report to the Department of Health and Human Service's Office for Civil Rights (OCR) in the event of a breach.
	
	• Third-Party Assurance:
	  ◦ Review the vendor's independent audit reports including financial audit opinions and SOC reports, measuring their security standards and practices against the OCR HIPAA Audit Protocol.
	  ◦ Understand the vendor's disaster recovery/business continuity plan and testing results.
	
	• Access Control:
	  ◦ Ensure the vendor restricts PHI system or software access to only those resources authorized to work on the coding engagement through assignment of Unique User IDs to track users. An emergency access procedure in the policies and procedures manual must be established that allows access to ePHI as needed in an emergency. Also, establishment of an automatic logoff to terminate electronic sessions after a predetermined time of inactivity is necessary, as is PHI encryption/decryption.
	
	• Physical Security:
	  ◦ Ensure the vendor restricts physical access so only authorized personnel have access to the building where data is stored or processed. Environmental controls can be enhanced with surveillance, monitoring and alarm systems, and policies for visitors.
	  ◦ Ensure CDOs or their designees have around the clock access to any of the vendor's production facilities anywhere in the world to inspect compliance with physical security requirements.

Financial stability	• Ensure the vendor can support engagement for the proposed term, which will likely include a spike in wages for trained ICD-10 coding resources.
Proven track record of service commitment Skills and experience to service CDO's needs	• Assess/measure the vendor's track record of service commitment from multiple perspectives: breadth and depth of outsourced coding services; coding accuracy and turnaround time; effectiveness of their quality assurance process; plan for transition to ICD-10; and demonstration of customer service. • Measure the quality and capacity of the resources proposed for the engagement: education and experience level of resources; professional certification of resources, etc. • Evaluate the vendor's ability to secure professionally certified coding resources if the CDO's policies dictate that coding shall be performed by certified resources. Assess the vendor's certification ability if offshore

	resources are being proposed, keeping in mind AHIMA stopped certification in many countries. • Require the vendor's coders to pass a coding test designed by the CDO, then use test scenarios that truly evaluate coding accuracy, query capabilities, and other key parameters. • Secure assurance in writing from the vendor that the named resources for the engagement (offshore or otherwise) have never been employed as bonded labor, as it may violate CDO's own principles and create a legal or public relations situation. This practice has long been prohibited under US law by its Spanish name "peonage." Workers in some foreign countries fall victim to debt bondage when companies exploit an initial debt the worker assumes as part of the terms of employment. • Ensure the vendor will not allow employees who have been listed in the Department of Health and Human Services' Office of Inspector General Exclusions Program—and therefore have been banned from participating in Medicare or Medicaid—to perform coding or other related services. • Establish standards, deadlines, and quality levels that need to be met for each type of coding service. Require that vendors' SLAs be backed fully by financial guarantees and follow customer service standards and operational metrics.
Account management plan	• Review the vendor's account management process and interview the proposed account manager and key service delivery people. • Secure named, dedicated coding and quality assurance resources so that they can be seamlessly integrated with the current coding and revenue cycle processes.
Comprehensive work migration plan	• Develop a joint migration governance process—form a steering group that has clinical and revenue cycle employee representatives, vendor representatives, and an outsourcing expert. • Ensure the vendor has a comprehensive, tested plan to guarantee a seamless and secure migration of operations and data to their production center. • Ensure the vendor absorbs and masters valuable experience and knowledge shared by the CDO's organization, including customer coding policies and preferences in accurate, thorough, and timely coding. • Require the vendor will fully conform to the CDO's policies, procedures, and practices at the onset of the engagement and provide regular, timely updates to these practices.
Pricing model	• Understand the vendor's pricing model—what the CDO is paying for, not paying for, hidden costs, price changes as needs scale up or down over time, and any future ICD-10 surcharges. • Develop and communicate with the vendor a comprehensive set of qualitative and quantitative SLAs. Require the vendor to provide pricing concessions or waived fees in the event the vendor misses any contracted service level commitment.

Outsourcing Coding Comes with Risks

Outsourced coding entails allowing access to patient records outside the CDO's physical facility. This causes:

- Physical and geographic separation of coding resources from clinical and revenue cycle resources
- Disruption and change to a facility's normal "query process," which hinders the ability to improve the accuracy of coding and support clinical documentation improvement (CDI) programs
- Complexity in maintaining integral elements by and between clinical documentation and the revenue cycle
- Greater data privacy and security concerns
- Reduced direct management oversight and control
- Process coordination and output turnaround across multiple time zones (differing length of work week and holidays may also cause issues)
- Differences in work culture
- Assumption of country risk, including exposures associated with political instability, exchange rate fluctuations, and disruption in operations

While spirited conversations occur across the nation on the shortage of and solutions for securing coding resources, CDOs are rapidly moving forward with the implementation of clinical information systems—which will further drive demand for accurate coding. With the country moving to ICD-10, issues associated with diverse disciplines—such as maintenance of the CDI program, clinical documentation systems and computer-assisted coding (CAC) systems implementations and processes, and coder-clinician query response interaction—will need to be accounted for when evaluating and deploying solutions to mitigate coding needs. Integration of those capabilities is also requisite to any third-party resourced assistance.

Because of HIPAA, the CDO and vendor should have a covered entity–business associate agreement in place before doing business. HIPAA-covered entities are liable for the acts of their business associate agents, in accordance with the federal common law of agency and HIPAA, regardless of whether the covered entity has a compliant business associate agreement in place.

For that cause alone, it is understandable why informed healthcare executives are tentative about moving forward with outsourced, remote coding propositions. Outsourcing of coding for some or all services is a big change with big implications for any organization. Outsourced, offshore remote coding increases the CDO exposure to risk. Hence, it is necessary to ensure safeguards are in place that can minimize CDO risk when considering the use of an outsourced offshore solution.

Questions to Ask When Considering Outsourcing

There are important discovery questions to ask—and receive answers—before any CDO agrees to let a vendor handle their core processes or operations. The answers to these questions must meet the CDO's strategic, operational, clinical, and financial objectives as well as support regulatory- and compliance-related obligations.

Deep collaboration with a trusted outsourced remote coding vendor can deliver effective coder-clinician query response interactions and efficient revenue cycle processes. An organization should trust a vendor will follow up on their promises, but verify if they have the ability to actually do so. However, the CDO's verification of the essentials of success—such as quality of resources, conducive business environment, effective production infrastructure, productivity and deliverable quality, and adherence to US laws and regulatory requirements—can be a difficult and arduous tasks when remote coding services are provided. The issues are likely amplified when coding is performed in a foreign country. CDOs must conduct thorough due diligence research of the prospective vendor, then leverage their initial contract to ensure the business objectives and regulatory requirements are met to the fullest extent. CDOs must appropriately modify the contractual terms at necessary intervals to maximize contract performance, gain expected benefits, minimize organizational risks, and address environmental, regulatory, and business climate changes.

Trust comes with satisfactory vendor responses to defined needs, and appropriate demonstration of capabilities when asked questions included in the table "Discovery Questions and Contract Considerations for Outsource Coding Vendors" appearing on pages 41 to 43.

The vendor's responses and promises should be incorporated into a written legal agreement. If a CDO has already operationalized an outsourced coding process, it is never too late to refresh the due diligence efforts, mitigate risks, and amend agreements.

Responses to carefully constructed questions will provide more meaningful insights into the vendor's business practices. Vendor responses are dependent on how CDOs raise and phrase their questions. For example, for risk mitigation questions, responses to "will you…" generally qualifies a large number of vendor potentials; "do you…" narrows down vendor choices; and "have you ever…" returns a small set of qualified vendor partners. This same patterned approach to questioning should also be used when talking to a vendor's references.

Verification of conformance to agreements over the term of the contract is an equally important element of the process. It would behoove CDOs to verify vendor responses to critical elements of success. For example, breadth and depth of services provided, such as remote resource support for coding adjacent CDI and CAC initiatives, quality of coding resources and deliverables, adherence to privacy and security standards, quality of the physical and technology infrastructure, financial stability, and customer orientation should all be verified as part of an organization's due diligence prior to signing a contract.

CDOs can best determine the verification approach that suits them. For example infrastructure verification may involve a trip to the vendor's locations, and may be done at stated intervals or ad-hoc, with or without notice. Resource quality verification may involve a review of credentials and test scenarios that truly evaluate the vendor's coders' accuracy, query capabilities, and other key parameters. Adherence to privacy standards may involve certification from the vendor that it has never used or stored patients' protected health information (PHI) in any form—other than to complete the coding transaction. A vendor's adherence to security standards may involve certification and physical verification of secure practices. Also, demonstration of business metrics and service level agreements (SLA) can be performed through interviews of current and previous vendor customers.

Enact Due Diligence When Choosing a Vendor

Outsourced coding can deliver results if deployed with care and managed well. Organizations should follow their due diligence to trust, verify, ensure conformance to contract terms, and mitigate potential risk, and then repeat the cycle as necessary.

Ajit Sett (asett@setthealthcareadvisors.com) is CEO of consulting firm Sett Healthcare Advisors, LLC. George T. Hickman (hickmag@mail.amc.edu) is executive vice president and chief information officer for Albany Medical Center. Karen Karban (karen.karban@mmodal.com) is the director of HIM product services at M*Modal.

Article citation:
Hickman, George T; Karban, Karen M. "Trust but Verify: Safeguards in Contracting for Outsourced Coding Services" *Journal of AHIMA* 85, no.6 (June 2014): 40-44.