Overseas Outsourcing: the Risk of Doing Business?

by Harry Rhodes, MBA, RHIA, CHP Jill Callahan Dennis, JD, RHIA Michael C. Roach, JD

In today's complex transcription environment, outsourcing is a standard business practice that requires managing some privacy risk.

Contract medical transcription has increased dramatically in recent years, and the issues surrounding it are becoming more complex, but the industry itself is not new. The first large contracts with transcription companies were signed around 1959, says Molly Malone, executive director for the Medical Transcription Industry Alliance (MTIA). "But even before the first large medical transcription companies began to appear on the medical transcription market in the late 1950s, there were thousands of cottage industry medical transcriptionists in place," Malone notes. Today, nearly half of transcription is outsourced to specialized vendors.[1]

Despite the large volume of outsourcing, the demand for transcription is outpacing the number of qualified transcriptionists. The search is leading overseas, beyond the reach of US laws intended to safeguard protected health information. For US health-care providers, who retain obligations at home for the confidentiality of patient data they send abroad, identifying the laws that apply to them is a vital first step. Providers should also be aware of contract provisions that can help protect them in the event of privacy and security breaches by their vendors or their vendors' subcontractors.

Experienced Help Wanted

Behind the increasing demand for transcription is the rise of the electronic health record (EHR). EHR systems are populated with digitized medical record reports, which are currently dictated and transcribed. As the number of EHR systems increases, the volume of transcribed medical reports needed to support these systems grows proportionally.

Technology may be the eventual solution, easing the demand for human transcription with new interfaces and devices. But even the current successful technologies still require the human touch. Voice recognition, for example, though accurate, still requires editing. Additionally, the difference between what is technically possible and what is locally feasible can be the difference between rolling out the latest labor-saving technology and continuing to employ transcriptionists per usual.

In the meantime, the escalation in demand has led to a labor shortage. "There are an insufficient number of qualified medical transcriptionists to meet the enormous demand," according to a MTIA press release.[2] The key word in this statement is *qualified*.

"There are approximately 300,000 to 400,000 medical transcriptionists in the current US labor force, with about 1,200 new medical transcription program graduates entering the work force each year," says Carrie Boatman, director of professional relations for the American Association for Medical Transcription (AAMT). "The problem facing employers is that the majority of transcriptionists graduating from a program require additional training before they can be truly productive."

Productivity in the current climate is measured against a high bar. Faced with large volumes of work, narrow profit margins, and strict quality standards, most employers trust their work to only experienced transcriptionists. Training staff is not a popular option. Training transcriptionists is an expensive proposition that can require six months to a year, says Boatman. Companies attempting to reduce or hold down costs are unlikely to budget the money.

Initially, outsourcing offered an immediate solution, allowing overwhelmed healthcare providers to reach beyond their immediate labor market and secure qualified transcription around the country. As the volume of work increased, healthcare providers and the transcription industry faced a limited national labor pool. The same technology that allowed providers to secure workers throughout the US was now used to cast the net beyond US borders.

The first contract transcription was sent overseas in 1994, according to Steven Mandell, DBA, JD, president and CEO of Heartland Information Services. Though no solid statistics currently exist, Mandell estimates that 10 percent of all contract transcription is now done overseas. Some estimates range considerably higher, based on the fact that many vendors do not advertise the ultimate destination of the work they subcontract.

Savings Unlikely Overseas

Unlike many companies that send work overseas, healthcare providers and vendors who offshore transcription are unlikely to see cost savings. "When you consider the investment in technology, the cost of telephone and Internet communications, staff training, management staff, travel, and proofreading costs, it is probably not less expensive to outsource medical transcription overseas," says Boatman.

US healthcare providers often assume that because Indian transcriptionists are paid less, the savings will be reflected in cheaper transcription contracts, says Mandell. "They don't consider all of the costs—they can only see what Indian transcriptionists are paid."

Indian medical transcription companies face many of the same problems as their US counterparts. The quest for enough qualified medical transcriptionists is universal. Price competition is intense, and competing based on low wages can make it a struggle to produce quality work.

In fact, from the Indian perspective, opening a medical transcription service is no guarantee of business success. "Statistically speaking, out of the 175 companies that were officially registered with the Indian government [in 1999] only about 10 percent are in existence today. And even these do not operate at full capacity," Vinayak Shankar, owner of a medical transcription company in Bangalore, India, wrote in 2000.[3]

Seeking transcription based solely on cost savings may be more than difficult, warns MTIA; it may threaten quality. "The pressure on reducing costs in healthcare tempts some institutions to look to outsourcing based on price only. This is dangerous," says Sean Carroll, current president of MTIA. "The real focus here should be on selecting quality partners. Simply put, sometimes this means paying more for the assurances of such a relationship. This is not a commodity business."[4]

Outsourcing and the Law

A number of laws and regulations affect healthcare organizations that outsource work involving protected health information. It is important for providers to understand which laws or regulations apply to their situations. Some of the key legislation is discussed below.

HIPAA

The privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA) impose certain obligations on covered entities that outsource work such as transcription. The privacy rule requires that providers put in place a business associate agreement with any person or company outside of their own work force who does work on their behalf involving "individually identifiable health information." The agreement must contain certain elements that safeguard the information shared with that person or company.[5-7]

HIPAA makes no distinction between domestic business associates and overseas business associates. The requirements apply equally, in that the obligation to enter into the business associate agreement belongs to the covered entity, not to the vendor. Nevertheless, a provider's approach to specifying the actual safeguards it requires may vary among vendors, depending on the perceived risks and the provider's policies.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, includes provisions that potentially affect how financial service organizations outsource work. Although most healthcare providers are not considered financial service organizations, the act does affect health insurers.

The act imposes obligations on a financial institution to make thoughtful outsourcing decisions. Financial institutions that outsource customer information must investigate the methods their vendors use to access and handle that information. In other words, the financial institution must assess and evaluate vulnerabilities to its customer information arising from the use of that outsourced vendor.

The financial institution also must determine whether it has exercised due diligence in selecting a vendor, critically evaluate what customer information should be shared, and ensure that the contract with a vendor requires appropriate measures to achieve adequate privacy and security of customer information. That contract should provide for reporting, enabling the financial institution to evaluate the service provider's performance and security.

California SB 1386

California SB 1386 became effective in July 2003, amending California civil codes 1798.29, 1798.82, and 1798.84. It applies to agencies, individuals, and businesses that conduct business in California and own or license computerized personal information.[8]

Vendors who handle information on California residents are affected by SB 1386. The bill specifies that an agency that maintains computerized personal information that the agency does not own must "notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[9] Companies employing outsourcing vendors to handle the personal information of California residents should ensure that provisions are in place that permit the required notifications.

European Union Data Protection Directive

The European Union Data Protection Directive does not apply directly to US-based healthcare organizations without operations in Europe. However, organizations that outsource functions to European vendors may be affected by this directive if the outsourcing arrangement involves what the directive defines as "human resources" data. As of October 1998, companies can be limited in transferring data out of the European Union Economic Area. The directive applies to information provided online by consumers, to corporate personnel and payroll information, and to any other personally identifying information. Healthcare organizations that transfer such data from Europe to the US should consider the impact of the EU directive on its operations.

India's Information Technology Act

India's Ministry of Information Technology and India's National Association of Software and Service Companies are involved in drafting a data protection law in response to privacy concerns of offshore clients. The law is reportedly coming in 2004 (but was not final at the time of publication). In the meantime, US healthcare organizations wishing to outsource functions to India that involve individually identifiable health information should be blending their security and privacy requirements into their outsourcing contracts and business associate agreements.

Identifying and Minimizing Risk

As complex and changing as the transcription market may be, it is also established business practice. With it comes risk associated with the outsourcing of any protected health information, within and without the country. Providers can manage that risk by being aware of applicable laws and seeking contract provisions that may better allow them to act swiftly to stop breaches of security by vendors and their subcontractors as well as better protect themselves should those breaches occur.

Self-Audits

A useful tool in gaining understanding of the many privacy protection laws and ensuring appropriate control of protected health information is the data protection audit. The first step of the audit is to ensure identification of, easy access to, and understanding of applicable laws. The second goal is to achieve compliance through established policies and procedures.

A data protection audit begins with a summary of applicable laws by jurisdiction. The provider then summarizes its existing privacy protection policies and practices. The audit should then seek to bring provider policies and procedures into compliance with the laws of the country in which it operates.

If policies and procedures are lacking, the audit should promulgate their development. Focus should be directed at correcting areas of deficiencies, and audit results should be reported to executive leadership as part of the organization's compliance program.

Contract Considerations

In their outsourcing contracts, providers also can consider a variety of practices to protect themselves from privacy and confidentiality breaches by their vendors or their vendors' subcontractors.

Providers should seek indemnification language in vendor agreements. The indemnification should protect the provider—its directors, officers, and employees—from suits by third parties (e.g., patients) who allege injury from misuse of the information by the vendor or its directors, employees, agents, or subcontractors.

Indemnification, however, is only as good as the financial resources of the entity or person giving the indemnification. Consequently, providers might require that vendors escrow funds for indemnification. Most vendors are likely to strongly resist and may refuse to put funds in escrow because escrowing funds for each of its customers will tie up a large amount of the vendor's money.

For vendors who resist escrowing funds, providers could require that the vendor post an indemnity bond. This would require the vendor to tie up less money than an escrow. However, such a contractual provision is still likely to be resisted vigorously by most vendors, as the purchase of the bond still carries cost for the vendor.

As an alternative to seeking escrowed funds or indemnity bonds, providers could require their vendors to maintain insurance that covers purposeful as well as inadvertent misuse of health information by the vendor's directors, employees, agents, and subcontractors. The provider should require that it be named as an additional insured and require the vendor to produce a certificate demonstrating that the provider is so named. Providers should also seek their own insurance that would cover misuse of health information by vendors and subcontractors.

Providers who want to avoid all risk associated with work performed beyond the jurisdiction of US privacy and security laws can consider seeking vendors that do not send work to employees or subcontractors located outside of the country.

Obtaining a judgment against an entity or person located overseas is difficult enough, but in situations involving the inappropriate release of information, the immediate objective is usually to stop or prevent a behavior, not obtain a judgment for damages or breach of contract. Even if a US court issues an injunction aimed at an individual located overseas, enforcing the injunction in a timely fashion will be practically impossible.

In spite of that difficulty, providers should require a contract provision that allows the provider to *obtain* (as opposed to *seek*) an injunction to stop an existing or threatened improper use or disclosure of health information. The difference is important, because normally certain conditions must be met before a court will grant an injunction. The target of the injunction (in this case it would be the vendor) often opposes the injunction in court, arguing that the necessary conditions have not been met. However, if the vendor has contractually agreed that the provider may *obtain* an injunction to stop certain behavior, the vendor will have a much tougher time raising objections.

The contract should also provide that the injunction can be obtained without waiving the provider's right to seek and obtain contractual or tort damages in addition to the injunction. Providers should further require that the contract state that the provider need not post bond in order to obtain the injunction; otherwise, the provider will have to post a bond with the court that issues the injunction.

To be sure, there are risks associated with outsourcing any functions involving patient information. Those risks may magnify when information crosses national boundaries. Nevertheless, outsourcing is likely to continue as a business strategy for many organizations. By being aware of the risks and the applicable laws and by taking extra care in contracting, HIM professionals can help their organization strike an appropriate balance between the risks and the rewards of outsourcing. ❖

Notes

1. "MTIA on Privacy Issue: Privacy and Quality Inseparable." MTIA press release, October 27, 2003, Seattle, WA.
2. Ibid.
3. Shankar, Vinayak. "Out of India." *MTIA Newsletter* 3, no. 5 (2000).
4. "MTIA on Privacy Issue."
5. See, e.g., Davino, Margaret. "Assessing Privacy Risk in Outsourcing." *Journal of AHIMA* 75, no. 3 (2004): 42–46.
6. See, e.g., Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health Information." 45 CFR Part 160 and Part 164, (a) and (e). August 14, 2002.
7. See, e.g., Department of Health and Human Services, Office for Civil Rights. "Health Information Privacy Frequently Asked Questions." Available online at www.hhs.gov/ocr.
8. A bill recently introduced in the California legislature (AB 2163—Confidentiality of Medical Records: Offshore Transcribing; Notice & Consent) would require California providers to first obtain the consent of the patient before permitting vendors to send medical record information offshore. Absent the consent of the patient, transcribing and/or processing of medical information would have to be done solely within the United States. The status and progress of this bill can be seen at www.leginfo.ca.gov/pub/bill/asm/ab_2151-2200/ ab_2163_bill_20040218_ introduced.html.
9. California Civil Code, Section 1798.29(b).

Harry Rhodes *(harry.rhodes@ahima.org) is director of HIM products and services at AHIMA.* ***Jill Callahan Dennis*** *(jdennis@healthriskadvan-tage.com) is principal of Health Risk Advantage in Parker, CO.* ***Michael C. Roach*** *(michael_roach@sbcglobal.net) is a principal in the law firm of Michael C. Roach & Associates, LLC in Chicago, IL.*

Article citation:
Rhodes, Harry, Jill Callahan Dennis, and Michael C. Roach. "Overseas Outsourcing: the Risk of Doing Business?" *Journal of AHIMA* 75, no.4 (April 2004): 26-31.