Assessing Privacy Risk in Outsourcing

Save to myBoK

by Margaret Davino

Healthcare providers can outsource transcription, but they can't outsource their obligation to safeguard privacy. Here's how to minimize risk.

Healthcare providers are faced with multiple pressures, many of them financial. The need for management to meet financial constraints often translates into a desire to contract with vendors at the lowest possible immediate cost, sometimes without thought as to the nonprice issues in a contract.

It is important to linger over the legal issues that may be associated with vendor contracts, especially with vendors that may subcontract portions of their tasks. The October 2003 incident in which a Pakistani subcontractor, in a dispute with a medical transcription company, threatened to release patient information on the Web provided a dramatic reminder of this. Provider and vendor liability has become even more important in light of HIPAA privacy and security regulations, which place an obligation on covered healthcare providers to ensure that their vendors safeguard confidentiality.

This article discusses specifically the considerations that should be given by healthcare providers when choosing a medical transcription vendor, and it offers tips to protect providers when entering into a medical transcription contract.

Transcription Outsourcing

Medical transcription is a vital part of healthcare operations. Accurate, timely transcription of daily notes such as operating room reports, discharge summaries, and radiology reports is essential for communication among healthcare providers. Transcription further factors into accurate coding and billing of services, satisfaction of regulatory requirements, and defense of medical malpractice suits. In recent years it has become important in the development of electronic health records.

Transcription is also a frequent candidate for outsourcing. Healthcare providers often contract out their transcription as a cost-saving measure (though cost savings may not be possible in all circumstances). Providers also choose outsourcing to meet staffing challenges posed by local labor markets, the need for specialized training, and their own staffing limitations.

Whatever the motivation for outsourcing, transmission of confidential medical information outside of facility walls places an obligation on the provider to ensure that the vendor protects the confidentiality of the information. HIPAA requirements make this issue more critical than ever before.

The case in which the Pakistani subcontractor threatened to release patient information illustrates how important it is for providers to choose vendors carefully to complete due diligence with regard to chains of subcontracting and to protect themselves contractually from liability for acts of the vendor or the vendor's subcontractors.

The above story started in fall 2003 when the University of California at San Francisco Medical Center (UCSF) forwarded a portion of its transcription work to Transcription Stat, a company it had used for two decades. Transcription Stat employs 15 subcontractors throughout the US to handle the large volume of files it receives daily from UCSF. One of those subcontractors, a woman in Florida, further subcontracted the work to a man in Texas named Tom Spires.

Allegedly unbeknownst to the other parties, Spires also employed subcontractors, one of whom was a Pakistani woman, Lubna Baloch. On October 7, 2003, UCSF received an e-mail from Baloch stating that Spires owed her money and would not respond to her. Baloch demanded that UCSF require Spires to pay her. If not paid, Baloch wrote, she would "expose all the voice files and patient records of UCSF . . . on the Internet."1 To show that she was serious, Baloch attached dictation reports from UCSF physicians regarding two patients.

One of the contracted parties involved ultimately paid Baloch, who then retracted her threat. Although the incident ended without a breach of patient privacy, the situation dramatically illustrated the risks for parties involved at all points in the chain. How can a provider best protect itself from a situation such as this?

What HIPAA Requires

The privacy regulations of the federal HIPAA law, effective April 14, 2003, were intended to ensure the privacy and confidentiality of personal health information. HIPAA's privacy rules apply only to healthcare providers, payers, and clearinghouses that are covered entities. Because the law does not directly apply to other parties that may handle medical information (e.g., transcription companies and other vendors), HIPAA attempts to stretch its coverage by requiring healthcare providers to take certain actions when entrusting medical information to vendors.

HIPAA requires that if a provider releases medical information to another person or entity to perform a function on the provider's behalf (the provider's "business associate"), the provider must enter into an agreement obliging the business associate to maintain the confidentiality of the medical information.

HIPAA's privacy regulations require that business associate contracts contain several specific provisions. The contract must specify the permitted uses and disclosures of information by the business associate. The contract also must require the business associate not to use or further disclose the information except as permitted by the contract and to use appropriate safeguards to prevent use or disclosure of the information other than as allowed by the contract. The contract must "ensure that any agents, including a subcontractor," to whom the business associate provides medical information agree to the "same restrictions and conditions that apply to the business associate with respect to such information." The contract must authorize termination if the business associate violates a material term of the contract.

When the HIPAA security rule goes into effect, medical transcription vendors will be covered as business associates under this rule also, because the security rule applies to electronic medical information, both in storage and in transmission. The rule requires that when providers contract with business associates who "create, receive, maintain or transmit electronic protected health information," the contract specify appropriate use of the information.

Additional security provisions may need to be added to business associate contracts with transcription vendors and other business associates that receive or transmit electronic information. For example, the security regulations require that any business associate shall "(i) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic protected health information that it creates, receives, maintains or transmits on behalf of the covered entity, as required by the security standards, (ii) ensure that any agent, including subcontractors to whom the business associate provides such information, agrees to implement reasonable and appropriate safeguards to protect it, and (iii) report to the covered entity any security incident relating" to the electronic information that the vendor maintains for the provider.

What Providers Should Determine

Providers should therefore determine how a medical transcription vendor maintains the privacy of medical information and how the vendor safeguards the security of electronic information. Providers should get answers to the following questions:

- Does the vendor have security safeguards for information that is maintained at the vendor's data headquarters (e.g., is each employee required to have a secure password)? Are voice files and data files maintained in a secure data safe?
- Is there an audit trail that shows who has accessed data in the vendor's archive system?
- How long are data files maintained, and are they destroyed after that period? Are voice files automatically deleted within a reasonable time after being transcribed? The provider may wish to specify that data is maintained only until the provider ensures that the transcribed report is in the medical record (e.g., no more than one year).
- Is electronic medical information transmitted from the vendor to the provider in a secure fashion—for example, through encryption?
- How does the vendor regulate provider access to the provider's directory on the vendor server? For example, is it safest to allow only one person authorized by the provider (e.g., the director of medical records) to draw data down from the transcription vendor's computer system?

- If the vendor employs home-based transcriptionists, does the vendor have policies to safeguard workstations? Are home-based transcriptionists allowed to store provider files on their home computers?

Minimizing Risk

Providers can consider a number of options when entering into a contract for medical transcription services. These options can clarify the mutual understanding of the contractual relationship, minimize the chance of a HIPAA or confidentiality violation, and ensure that the provider will be able to take appropriate action should a vendor fail to meet required standards.

1. Ensure that the contract with the medical transcription company obligates the vendor to not only maintain confidentiality itself, but to require any person or entity to whom the vendor sends information to maintain confidentiality and security of information. The vendor should require that the person or entity comply with all of the obligations of the vendor under the vendor's business associate agreement with the provider.

   In the UCSF case, the transcription vendor, the first subcontractor, and second subcontractor were simply intermediaries. That realization makes a provider wonder how many transcription vendors operate by simply contracting with another party whose cost is low enough to allow the first vendor to skim off a profit, and so on down the line until the only person left to do the work is someone whose wages are below those livable in the US. It is difficult to ascertain how HIPAA's privacy or security requirements can be satisfied if a transcription company is simply a pass-through: can anyone identify who has the data, how it is stored, or where it is? Nevertheless, the HIPAA rule assists providers by making clear that vendors are responsible for the privacy and security of the data given to them.

   The obligations of both provider and business associate become further complicated if some of the parties receiving information are not located inside the United States. Entities not domiciled in the US may not be subject to, or even aware of, US laws.

2. Require indemnification from the vendor for any breach of the contract (including confidentiality), not only by the vendor but by any of the vendor's subcontractors or entities to which the subcontractor may send information.
3. Consider placing restrictions on the subcontractors that a vendor may use; for instance, explicitly requiring that any subcontractor receiving medical information from the vendor be physically located in the United States and that, in addition, the vendor's subcontractors be explicitly prohibited from sending any of the provider's information outside the US. Although this will not obviate the problems that can occur if a subcontractor isn't paid and threatens release of information, for example, it will ensure that any such subcontractor is subject to US law and may be less likely to make such threats. Also, providers can consider asking vendors outright for a full disclosure of subcontracts.
4. Consider using a medical transcription company that does not subcontract any work at all. Some vendors are staffed with full-time employees who receive benefits, and some offer incentives to staff for meeting high performance standards. Some vendors assign transcriptionists responsibility for a single client, fostering familiarity with the client's transcription needs. Such vendors may charge a premium for that level of service, but providers may want to balance that cost with the potential benefits of a stable, dedicated staff.
5. Consider whether the transcription company is making investments to obtain and retain the provider as a customer. Is it purchasing computers and equipment for use on the account, or is it simply subcontracting all work and keeping a percentage of the fee ? The answer gives the provider a clue as to how much the vendor values the relationship and how carefully other contract terms should be reviewed.
6. Ensure protection by including specific performance standards in the contract. These should include turnaround time, error rate, and template consistency (so that the documents follow a standard format). Not only are written performance standards important to give the provider the ability to terminate the contract if standards are not met, they also can help identify hidden costs. Although one vendor may appear to be less costly than another, does a high error rate require the provider to allocate time from other employees to review, edit, and correct the vendor's work?
7. Weigh the cost of training staff regarding confidentiality. HIPAA requires that all persons with access to personal health information receive training on the confidentiality requirements of the law. In addition, laws in some states require additional staff training for specific situations, such as New York's AIDS confidentiality law. It can be easier for the provider to place the burden of training on the transcription company.
8. Ensure that the contract contains the protection terms standard in any contract: (1) the ability (of both parties) to terminate the contract for cause (e.g., failure to comply with the terms of the contract) and not for cause (if the vendor has made a substantial capital investment in the provider's account, this clause may only be agreed upon if the provider

takes some responsibility for the investment); (2) an appropriate length of time for the contract; (3) inability of the vendor to assign the contract without the provider's permission; and (4) a requirement that any claim be brought in the state in which the provider is located.

In the wake of the UCSF case, a California state senator discussed introducing legislation that would prohibit provider and payer organizations in California from sending confidential medical information outside of the United States for transcription or other outsourced data processing activities.

Such a law would ensure that all vendors and their subcontractors are subject to US laws, but it would not alter a provider's core responsibilities when transmitting confidential records to a vendor. Meeting responsibilities and minimizing risk will still require asking the right questions, weighing the options, and establishing an appropriate business associate agreement.

Note

1. Lazarus, David. "A Tough Lesson on Medical Privacy: Pakistani Transcriber Threatens UCSF over Back Pay." *San Francisco Chronicle* (October 22, 2003). Available online at http://sfgate.com.

Acknowledgement

The author wishes to thank Marilyn Grebin of Silent Type, Inc., for her assistance in the writing of this article.

Margaret Davino *(mdavino@kbrny.com) is an attorney with Kaufman, Borgeest & Ryan, New York and New Jersey, specializing in health law. She was formerly general counsel of St. Vincent's Hospital in Manhattan and of St. Joseph's Hospital in Paterson, NJ.*

Article citation:
Davino, Margaret. "Assessing Privacy Risk in Outsourcing." *Journal of AHIMA* 75, no.3 (March 2004): 42-46.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.