3 Vendor Relations and Privacy

By David B. Nelson, CHRC, CHPC CISSP, CIPP/G

Introduction

Vendors play a critical function in aiding health care entities to deliver services. The vast array of what vendors might supply ranges from vital services such as physicians, temp nurses, billing or research services right down to educational pamphlets, paperclips and jugs of water for coolers. The range of services, between relatively simple to extremely complex, is reflected in the portrayal of the business relationship.

But problems can arise when products aren’t delivered in a timely fashion, the wrong quality of product is delivered or additional requested items are provided but with exorbitant additional fees attached, or our clients’ privacy rights are violated.

The privacy impact from vendors depends, too, on whether they just walk in and drop off a case of alcohol wipes, work on site extracting information from an electronic health record for quality assurance or provide legal services from their home office in another state. The vendor who is required to enter sensitive areas to provide services or supplies requires a different level of privacy controls compared to the vendor who can do a drop and run from the loading dock. Another vendor who provides services elsewhere and never comes on site has other privacy risks. The variations must be accounted for in the principal control tool: the contract.

Disclaimer. This chapter is not a legal treatise on contracts, but simply
intended to help the privacy professional who may have only limited contract experience to focus on the construction of a contract and the issues that may arise in the vendor relationship. This chapter should help the privacy professional understand how to fit privacy concerns into the contract. Your counsel may have an opinion that varies on contract construction and the usefulness of some ideas expressed here. You should consult with your counsel and follow their advice.

This chapter will focus on suggested privacy controls that could be put in place in the contract and the purpose those controls serve in developing and maintaining vendor relations. Some pitfalls will be identified and guidelines will be provided for how to design the relationship (contract), monitor it while in process, and then close it so that both parties are confident that delivery met expectations.

Pre Contract Assumptions

Developing the vendor relationship starts with the assumption that a contract will be used for most vendors. Sometimes it will be your contract and sometimes it will be the vendor’s contract. Most legal counsels would prefer to be the contract originator, as the originator has substantially more control of the relationship; but contract origination may be out of your hands. In either case, the pre-contract work is the beginning of the relationship and needs to account for the foreseeable privacy issues.

While a bit simplistic, it needs to be said that both parties to a contract should understand that the other party is subject to varying laws and regulations. In short, each party needs to understand that the other must live up to certain legal mandates. The reasonably competent privacy professional should understand both parties’ legal mandates. This may mean the health care privacy professional will have to go outside of their comfort zone (HIPAA, 42 CFR Part 2...) and learn the basics of other privacy laws (SOX, GLB, FTC Red Flags...).

Mutual Understanding

The first piece to grasp is that contracts are about creating mutual
understanding. This concept is vitally important, as all parts of the contract are put in place to enhance understanding, which supports a successful business relationship. The contract is not just another business hurdle. Contracts will incorporate many parts of your business operations and how they interact with your contractors. For example, topics like risk management, IT implementations, strategic planning, business continuity, and accounting requirements are just some of the issues that may have to be addressed in a contract. Implementing appropriate contractual measures mandates mutual understanding.

Privacy is the framework we operate under, and the laws and regulations tells us what we must protect. Yet specific security features will usually be the focus in a contract, as they support the privacy mandates. Privacy tells us what to protect, and security tells us how to protect it. It could be said that all privacy mandates and standards are implemented through security measures. But some concepts, like HIPAA “minimum necessary,” do not always have a security solution. Contracts can quote HIPAA, or other privacy laws, but unless specific implementation steps are included, a gap in understanding is created. Gaps equal increased risk.

Consider:

- Access into your building
- Where the contractor can go while in the building
- Where the contractor is forbidden to go
- Information the contractor should have access to
- What the contractor can do with information
- What the contractor cannot do with information.

Each of these represents a risk to the privacy profile. We express our expectations of vendors and the possible impact to our privacy program through our contract language.

Keeping all this in mind, no one wants a nine-hundred-page contract. The privacy professional must ensure that the contract supports the privacy profile. In order to make the concepts of contracting more understandable, the
document can be separated into two parts. The first part is referred to as the boilerplate and the second part contains any specifics that must be accounted for.

The boilerplate is the part of the contract that has standard clauses that define all contractual relationships. The boilerplate may have indemnity clauses, insurance requirements, term and termination and anything that would be considered a minimum standard in all contracts for your entity. Each entity has a slightly different list of boilerplate clauses.

To try and describe everything in a boilerplate contract would be onerous. So for the boilerplate, we must choose what is generally true for our entity in most situations. Your counsel has probably done this already. When a privacy item must be detailed because the implementation must be supported in a particular way, we come to the privacy clauses.

A note of caution: while boilerplate is in theory a designation for all contracts, you should ensure that each of the boilerplate clauses is appropriate. For example, you may have a HIPAA Business Associate (BA) language clause as part of your boilerplate or optional addendum. One item that is usually included in the BA language is the client’s right to request a copy of their information. In some contractual relationships, like contracted QA/QI activity, the contractor would never supply a copy of a record to the client because they have no relationship to the client. The client access section should probably be cut. Contracts are about mutual understanding and having language that does not apply detracts from the understanding. It would not be appropriate to say “just ignore what doesn’t apply,” as the contractor may apply the same caveat to critical portions of the contract.

The second part of the contract could be considered adjustable and contains those clauses that change or are added for the specific contract. While sometimes only a few clauses are in this section, like scope of activities and pay schedule, this part of the contract is where the privacy professional can clearly outline privacy impacts from the vendor’s services.

Another concern in your relationship to the vendor is that vendors are not “partners” in your enterprise. This is true regardless of what the contract states they will provide, if you pay them or they pay you. Ethically a separation must be made so that this separation is clear to both parties. If the vendor is treated as a partner, deferred to as if they are a partner, referred to as a partner,
it could lead to tensions in relations as the expectation of a partner is different than those of a vendor. Too often contractors in the “partnership” situation believe themselves to be indispensable to your organization with inalienable rights. They can become hostile when relegated, appropriately, to their role or called to task when they violate regulations that your entity must abide by and were notated in the contract.

A weak privacy profile characteristic that shows up in contracts is when the contract says “fully HIPAA compliant” either as a claim by the contractor or as a mandate from the contract originator. Does the statement mean anything in relationship to their role? Does it mean they are, or are to be, complaint with 5010 format? Will they do a full-blown risk analysis for their product in your environment? Can they capture disclosures electronically? Vendors may have done everything possible from their end to be HIPAA compliant, but until they account for your business operations it is just a marketing phrase. On the opposing side, the phrase has doubtful value as a mandate without describing exactly what it means for your vendor. Undefined phrases about the privacy compliance are dangerous, as they lead to misunderstanding and that leads to increased risk.

Achieving mutual understanding is the goal and it takes work on both parties’ behalf to ensure the expectations meet delivery.