

Safe Harbor

Addressing Security Issues in IT Contracts

Security means different things to different people. In health IT, security generally means protecting against loss or damage to systems, data and information of the IT user. The type of information and data could be any sensitive, confidential or proprietary data, including health-related patient information. But it also includes sensitive business-related information, such as that which gives an IT user a competitive advantage in the marketplace. This article provides an overview of examples of ways to address security issues in an agreement with an IT vendor.

SOFTWARE AND SYSTEM SECURITY

IT users can protect software and systems from damage by including warranties in the agreement. One such warranty protects the user against disabling codes—also called trojan horses or trap doors, among others—which are intentionally inserted into programs by the vendor. This “back door” access allows vendors to easily de-activate or disable software in the event of a dispute with a client. There have even been cases of unscrupulous vendors using these codes to earn additional fees to correct a software “problem.” Including such as protection in a warranty ensures that the IT user is protected from these codes.

Another warranty that is helpful in this regard ensures that the vendor has made certain agreed-upon efforts scrub the soft-

ware of viruses. Though most vendors will not guarantee their software to be “virus-free,” many agree to scan software for viruses prior to shipment, including any updates or upgrades provided under maintenance and support.

DATA AND INFORMATION

Most IT contracts contain a provision that can be used to protect general confidential or proprietary information of the user. However, many standard IT vendor contracts define “confidential information” in a manner that best protects the IT vendor’s interests. For example, a standard IT vendor contract may define “confidential information” as the terms of the contract, the software and related items being provided and any other information the IT vendor provides to the IT user.

Users need to expand this definition to include *information* it wants to protect. The IT user should consider that IT vendor personnel may be onsite and have accidental or unintended access to information. For that reason, if “confidential information” is defined as information which is marked as “confidential” or “proprietary,” the IT user may not be adequately protected. This provision also should require that, to the extent possible, the parties will return the other party’s confidential information at the conclusion of the contract.

Another method of providing security by way of the IT contract is to include a provision that gives the IT user the right to use a screening process and to perform background checks for any individual performing services for the IT vendor under the contract. It is important to be able to identify individuals who may be a potential security risk and have the right to remove and replace such individuals. Background checks may involve additional legal pitfalls and should be developed in conjunction with legal counsel.

Many IT vendors will require remote access to the IT user’s systems to perform diagnostic and corrective services. The IT user should include contractual provisions making the IT vendor’s access to its systems subject to the IT user’s security policies and procedures. Of course, this provision requires that the IT user actu-

ally develop clear policies and procedures that the IT vendor can follow. Often, the IT vendor will want to review these policies and procedures during the negotiation of the contract.

In the event the IT vendor has actual physical possession of the IT user's confidential or sensitive data, the IT user can reduce the risk of loss or damage to the data by having the IT vendor agree in the contract to the security measures that the IT vendor will employ with regard to such information. Examples include authentication/password protection, firewall protection, data encryption, intrusion detection and countermeasures, daily backup, archival in a secure facility, and disaster recovery measures. The IT user may even want the contractual right to periodically tour the IT vendor's facilities to ensure these security measures are being utilized. In addition, the contract should require the IT vendor to give the IT user immediate written notice in the event of a breach of the confidentiality, integrity or privacy of the IT user's data. The IT user should also request and review the IT vendor's disaster recovery plan and consider including it as an obligation within the contract. Services to restore data lost as a result of the IT vendor's breach of these provisions should be at no addi-

tional charge. The IT vendor should also be required to periodically provide a copy of the data to the IT user to minimize any loss.

Of course, one of the most sensitive areas in the healthcare industry regarding security concerns patient-related data. In the event the IT user is a covered entity under HIPAA and will be disclosing patient-related data to the IT vendor as part of the transaction, the IT user must execute a business associate agreement addressing the privacy of such information, as required by HIPAA. If the IT vendor will possess or store patient-related information, the business associate agreement must also address the security of such information, as required by HIPAA. The determination as to whether a business associate agreement is required is simplified for the purposes of this article. The determination should be made on a case by case basis with the advice of legal counsel.

The IT user should consider further protecting itself by requiring the IT vendor to indemnify the IT user for security breaches. For example, in the event the IT user incurs a fine, penalty or other fee imposed by a state, federal or local agency due to the IT vendor's failure to comply with a security provision in the contract,

the IT vendor would be required to pay the IT user the sum of such imposed fine, penalty or other fee, and indemnify and hold the IT user harmless from any action or claim related thereto.

IT users can protect software and systems from damage by including warranties in the agreement.

There are many ways a healthcare company can minimize loss or damage to its data, information, and systems. Negotiating contractual language regarding security issues not only provides legal recourse in the event of a security breach, it also fosters discussion about each party's expectations and capabilities regarding security issues before the parties have legally committed to the transaction. Such discussions may uncover security issues that were not previously apparent. **JHIM**

Robert Doe, Esq., is a founding member of the law firm Bonnabeau, Salyers, Stites, Doe & Andresen (www.bssda.com) located in Minneapolis, MN. Mr. Doe has extensive experience preparing, reviewing and negotiating IT contracts. He can be reached at rdoe@bssda.com or 952-548-6064.