FATAL HEALTH CARE IT DECISIONS TO AVOID

These tips can help you draft air-tight contracts when dealing with information technology vendors.

BY JEFFERY DAIGREPONT

When it comes to preventing mistakes, health care organizations are held to some of the highest standards of any industry. There are entire government agencies devoted to enforcing policies and performing audits with the intent to reduce the risk of mistakes. However, when it comes to information technology (IT) platforms within health care, it is basically a buyer beware market with many broken promises. While vendors must adhere to certain compliance standards, those standards rarely address defects and deliverables. For example, most vendor contracts allow for warranty exclusions or offer only a limited warranty. In most cases, the warranty may even expire before the software is installed.

We have all heard horror stories of the Department of Justice (DOJ) fining electronic health record (EHR) vendors for false claim violations, often related to the misleading capabilities required for EHR incentive programs. We all know of a practice or a provider who purchased defective software or had their EHR discontinued shortly after the purchase. And we have all seen the headlines of cyber security breaches, often due to vendors that do not properly protect their software. These issues have become so prevalent that, a few years ago, the DOJ stepped up its efforts to audit vendors.[1]

Health care organizations rely on technology for day-to-day operations, accounting systems, appointment calendars, EHR systems, and countless other systems. Decisions related to which vendors/products to invest in have organization-wide consequences and should be dealt with carefully. Practice leaders should conduct careful research to avoid future problems with the health care technology of choice.

This article highlights some of the most common IT contracting mistakes and provides tips to help retina practices avoid or correct these issues.

BUYING DEFECTIVE SOFTWARE

Software defects range from minor glitches to major liabilities. Most defects can be corrected, or workarounds can be developed. However, in cases where the defect creates a threat to security or patient safety or is a liability to the practice, the vendor must address the defect immediately or the practice must discontinue using the software. Knowingly using defective software can

AT A GLANCE

- While vendors must adhere to certain compliance standards, those standards rarely address defects and deliverables.
- When buying software, the vendor contract should include language clarifying who is responsible for software defects and any resulting liabilities.
- If a vendor fails to maintain its compliance certification, the practice should have the right to terminate without penalty.
- Vendor contracts should stipulate that a practice is entitled to a prorated refund if the system is discontinued during the term of the contract.

create unwanted liabilities for the practice, as it may be considered negligence.

Common examples of fatal software defects include any malfunction that might negatively affect patient care, patient privacy, or security. A defect may not always be software related; it may be related to workflow, system design, or usage. The most secure system in the world cannot stop employees from sharing their passwords, but the software should be able to help manage and detect these threats. Software defects should be confronted immediately, as there could be additional risks associated with knowing about a threat but not acting. Vendors should also be held accountable to correct these issues at no cost to the practice.

When buying software, the vendor contract should include language clarifying who is responsible for software defects and any resulting liabilities. In extreme cases, software has been known to contribute to the harm or death of patients.[2] For example, in a recent EHR launch for the Veterans Affairs, four patients died before clinicians discovered that the problem was related to a software glitch.[2] Among other technical issues, the system was sending orders for speciality care and medications to an unknown location; it was also failing to reroute no-shows to the scheduling system—all of which delayed care.

The method for correcting defects will vary, but the first step is to document the problem, take screenshots of the defect, formally notify the vendor about the defect, and immediately discontinue any related usage that may create risk. In cases of security vulnerabilities, the system may need to be taken offline until the defect is repaired.

Contracting tip: Add language to clarify that defects not corrected within 30 days will result in a suspension of the practice's financial obligations. If not corrected within 90 days, the practice will have the right to terminate without penalty.

COMPLIANCE CONCERNS

Most practices invest in health care technology with the expectation that the software meets national standards or federal mandates, particularly if it's listed as an approved vendor by the Office of the National Coordinator (ONC) for Health IT. But what happens when the vendor fails to develop its product under ONC guidelines? If the technology does not have the system capabilities to earn EHR stimulus incentives, the vendor may be disqualified as an approved EHR by CMS. CMS will only issue incentives to practices who use CMS-approved vendors, commonly referred to as certified EHR technology.[3] Moreover, CMS may enforce penalties for not complying with these mandates by reducing Medicare reimbursement by as much as 9%, according to the AMA.[4,5]

Many vendors have anywhere from five to 10 different versions of their software in a solution stack, but only certain versions meet the standards. Far worse, a certified product today may not stay certified in the future.

We recommend first determining if your software meets the compliance standards by ensuring it complies with the HIPAA Security Rule and HIPAA Privacy Rule. HIPAA establishes a national standard to protect health information and outlines how sensitive information should be handled for storage, transfer, and communication. Elasticity and adaptability are built into these guidelines to fit health care organizations of various sizes and structures.

Your software implementation team should fully understand compliance regulations to ensure that the policies and procedures surrounding the use of the technology are appropriate for the size and structure of the practice and compliant with both the privacy and security rules.

The next step depends on the type of software. If the solution must meet meaningful use, which will soon become part of the Merit-Based Incentive Payment System and the Medicare Access and CHIP Reauthorization Act, it will need to meet certification by the ONC.

Common software compliance slip-ups occur when a vendor meets a certification one year but loses it the next. Vendors may fail to meet new standards or release software that creates challenges to meeting new standards. Due to stiff competition, some vendors will offer bold compliance performance promises by agreeing to pay back providers who fail to achieve compliance using their software. While they have no way of guaranteeing a user will comply, vendors will guarantee that their software will meet standards, or they will pay the penalty.

Penalties for Noncompliance

If your practice is noncompliant, you can resolve the issue by establishing corrective action. However, if this action is not implemented immediately, you may face financial penalties. In the case of HIPAA, there are two penalty levels: civil and criminal.

Civil is applied if the individual or practice was not aware of the violation, if there was reasonable cause for the violation, or if it was willful neglect. Civil penalty fines can range from $100 to $50,000 per violation.

Criminal penalties are more severe and can range anywhere from $50,000 and 1 year in prison to $250,000 and up to 10 years in prison. In the case of meaningful use, the penalty would be a reduction of Medicare compensation, which can be as high as 9%. Note that participation in meaningful use is not mandatory for

EVERY CONTRACT SHOULD HAVE A WARRANTY THAT REQUIRES A VENDOR TO CORRECT DEFECTS AT ITS EXPENSE, AND YOU SHOULD NEVER SIGN A CONTRACT WITHOUT BEING ENTITLED TO FUTURE UPGRADES AND NEW RELEASES.

practices that do not see Medicare patients, whereas HIPAA is required by law regardless of the payors.

Contracting tip: Language should stipulate that the practice has the right to terminate the contract without penalty if the vendor fails to maintain its ONC compliance certification.

PREPARATION IS KEY

Technology is constantly improving and being replaced by newer and better models. When new software is released, older programs often are no longer supported and are not eligible for upgrades. In short, you're on a sinking ship and you will need to replace the system. Vendors rarely publicly announce when they plan to commercially discontinue a system, but the warning signs can include the following:

- The vendor stops appearing at industry conferences.
- The vendor acquires a second, more modern, platform touted as a way to "improve its offerings" but is, in reality, a stall method.
- The vendor does not have any job postings or is in a hiring freeze.
- Vendor executives are updating their LinkedIn profiles.
- Vendor executives are selling their stocks/shares.
- The customer support is in decline.
- Updates and new releases are scarce.
- You have not received any new features or enhancements.

IMMEDIATE ACTION

When a vendor discontinues a product, software updates are no longer available, and the product becomes more susceptible to cybersecurity threats and glitches. This can cause your practice to fall out of compliance, be subject to penalties, and be prone to interruptions in workflow due to slow or malfunctioning software. Usually, software innovation and new features follow updated regulations. For example, a patient portal is required for meaningful use stage two. Your initial software version may not include a patient portal, and your vendor may or may not provide the portal in the next release at no extra charge. Your contract should state that the vendor is expected to provide the system functionality required to stay in compliance at no additional cost to you.

HOW TO JUMP SHIP

If your system has been discontinued or is nearing discontinuation, immediately begin the search for a more current product. Although the system will still function and you may see no immediate changes in your day-to-day practice, your data will no longer be safe from cyber-criminals. No one enters a vendor partnership expecting discontinuation, and most are surprised to find out how little protection they have under these circumstances.

Many systems are now hosted via cloud computing, which means there is a possibility that system access could be discontinued with no way to operate independent of the vendor and the discontinued product. Practices should have a clear understanding of what to expect upon termination and/or in the event of product discontinuation. More specifically, you must be aware of the process of migrating data to another solution in such an event.

Contracting tip: Stipulate that the practice is entitled to a prorated refund if the system is discontinued during the term of the contract. Require a no-cost system conversion if the vendor acquires a new platform to replace the one initially purchased. Ensure the vendor contract includes the requirement for an advance end-of-life notice. Vendors typically know months, or even years, before they make the decision to announce the end of life for a product. You can also request after-life support (the industry standard is 3 years after the product is commercially discontinued).

THE ONE-OFF TRAP

A one-off is when you cave to the pressures from a department or individual who needs a specific IT solution to fill in gaps around an existing solution. One-offs might offer some temporary relief, but they create fragmentation

and make it more difficult to evolve into a more enterprise ecosystem. You will also run into application retirement challenges and the need to properly archive and store data for a system only used to fill a temporary gap.[6] For example, practices may use low-cost reporting tools beyond what is available in the native EHR, a patient check-in application, or both. This increases your security risk and adds challenges should the practice need to retire these third-party applications. It is always best to first explore any potential workflow workarounds or behavior changes for practice employees who feel they require an individualized solution not provided by the existing technology.

Before adding a one-off solution to your practice's suite of technology, make sure it can coexist within the existing environment. If you don't, you may end up with a manual workaround or expensive interfacing that requires management for the entire life of the product. In addition, be sure the vendor offering the one-off takes full responsibility for its compatibility.

Contracting tip: Secure a termination right if the one-off product is not compatible or does not work as promised. Practices can require an acceptance period, which states that you do not accept financial responsibility until you can test and verify that the one-off application works as promised.

GOING LIVE WITH AN INCOMPLETE SYSTEM

The pressure to go live on a new system is often driven by a vendor that is trying to recognize revenue by burning through the hours in the budget so it can get to the next install. In some cases, the system may not be properly tested before going live. As a result, physicians are frustrated by a bad first experience or experience backsliding in workflow efficiencies.

To avoid this pitfall, adopt a DBVT plan: design, build, validate, and test. For example, design your order form, build the form, validate the form with end users, and then test the form with end users. Ending the process with validation and testing will help you avoid moving forward with an incomplete system design.

Office of the National Coordinator Certification

Not sure if your vendor is certified? Follow the QR code or visit **bit.ly/3qESHnq** to access the list of products certified by the Office of the National Coordinator for Health IT.

Contracting tip: Add language to each vendor contract to clarify that the practice will not accept the full financial obligations until testing is completed and the system is live. We recommend the following payment terms as a hedge against having an incomplete system at go-live:

- ***20% at contract signing***
- ***20% at project kick-off***
- ***20% at installation***
- ***20% after testing***
- ***20% 30 days after go-live***
- ***Subscription services start at go-live***

CONTRACT WITH CARE

Retina practices can avoid the fatal health care IT decisions discussed here by modifying the agreement with the vendor during the contracting phase. For example, every contract should have a warranty that requires a vendor to correct defects at its expense, and you should never sign a contract without being entitled to future upgrades and new releases. Although the decision to add one-off technology may not be up to you, always discuss the unintentional consequences of this approach before signing the contract.

Contract reviews should be standard to ensure your practice is protected from these IT pitfalls. These reviews should be conducted during the contracting phase before anything is signed and agreed to, but they can be completed at any time to help inform improvements. Practices should consider partnering with a health care advisory firm to review vendor contracts and provide guidance on how to minimize these fatal mistakes. Patient safety, practice efficiency, and data security depend on it. ■

Author's note: To inquire about Coker's free EHR contract review, send a request to lrowlands@cokergrou.com or jdaigrepont@cokergroup.com.

1. Sullivan T. DOJ will probe more EHR vendors for false claims, sources say. Healthcare IT News. June 2, 2017. Accessed June 13, 2023. www.healthcareitnews.com/news/doj-will-probe-more-ehr-vendors-false-claims-sources-say
2. Diaz N. VA says 4 deaths linked to its Oracle Cerner EHR system. Becker's Health IT. March 17, 2023. Accessed July 1, 2023. www.beckershospitalreview.com/ehrs/va-says-4-deaths-linked-to-its-oracle-cerner-ehr-system.html
3. Certified EHR technology. Centers for Medicare and Medicaid. Accessed July 1, 2023. www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification
4. Merit-based incentive payment system. HealthIT.gov. Accessed July 1, 2023. www.healthit.gov/topic/federal-incentive-programs/MACRA/merit-based-incentive-payment-system
5. Merit-based incentive payment system (MIPS). American Medical Association. Accessed July 1, 2023. www.ama-assn.org/system/files/medicare-basics-mips.pdf
6. Harry G. Options for application retirement in an age where critical patient data resides in legacy systems. Coker Group. September 2016. Accessed June 13, 2023. bit.ly/3N1aZqB

JEFFERY DAIGREPONT
■ Senior Vice President, Coker Group, Alpharetta, Georgia
■ jdaigrepont@cokergroup.com
■ Financial disclosure: Employee (Coker Group)