Five Fatal Healthcare IT Decisions to Avoid

White Paper

Coker GROUP
Business Advisors for the Healthcare Industry

JEFFERY DAIGREPONT
Senior Vice President

December 2016

CONTACT

For further information about Coker Group and how we could be of assistance, call 800-345-5829 x137 or visit www.cokergroup.com.

TABLE OF CONTENTS

Abstract: The healthcare industry is held to a higher standard than other industries when it comes to the use of technology. Further, mistakes can result in greater consequences. Healthcare organizations rely on technology for day-to-day operations and functions, and the decisions on which vendors and products to use have organization-wide consequences.. Appropriate research should be conducted and decisions should be dealt with carefully to avoid future problems with technology. This paper highlights five healthcare information technology (IT) decisions that can be fatal to your organization, and it provides essential information to avoid these issues or correct existing concerns.

Key Words: Healthcare Information Technology, IT Decisions, EHR Systems, Compliance Standards, Non-compliant Software, EHR Incentive Programs, Meaningful Use, Defective Software, DVBT, One-Offs.

INTRODUCTION

The healthcare industry does not get a pass on making mistakes with their technology. Rather, healthcare is held to a higher standard than other industries, and the consequences are much greater when blunders occur. Healthcare organizations rely on technology for day-to-day operations, accounting systems, appointment calendars, electronic health record (EHR) systems, and many other functions. Decisions on which vendors and products to use have organization-wide consequences and should be dealt with carefully, based on the appropriate research to avoid future problems. This paper highlights five healthcare information technology (IT) decisions that can be fatal to your organization. It provides essential information to avoid these issues or correct existing concerns.

BUYING DEFECTIVE SOFTWARE

When problems arise, they may not be your fault, yet the resolution is yours to address. Defects in software range from minor glitches to major liabilities. Most defects can be corrected or workarounds developed to counter the obstruction. However, in cases where the defect creates a threat to security, patient safety, or liability to the organization, the issue must be addressed immediately, and/or the software use discontinued. An example of liability for using faulty parts or products is Toyota's sticking gas pedals and the company's subsequent inaction to the problems.[1] Issues cannot be ignored or hidden.

[1] http://abcnews.go.com/Blotter/toyota-pay-12b-hiding-deadly-unintended-acceleration/story?id=22972214. Accessed December 15, 2016.

The Defects

Typical examples of fatal software defects include any malfunction causing an adverse impact on patient care, patient privacy, or security. Defects may not always be software related. The hindrance could be workflow, system design, or usage. Although software should be expected to help manage and detect these threats, the most secure system possible cannot stop two employees from sharing their passwords, for example. Problems of software defects should be confronted immediately as there could be additional risk associated with knowing but not acting on a threat. Vendors also should be held accountable to correct these issues *at their cost*.

Things to look for When Buying

When buying software, the contract always should include language stating who is responsible for software defects and any liabilities resulting from them. In some extreme cases, software has contributed to the harm or death of patients. A *New York Times* article reported on incidents of harm done to patients due to computer errors in the complex machinery used for radiation treatment. In one of the cases specified, the software was feeding an overdose of radiation to a cancer patient.[2] The patient died as a result. Although the article cited 1264 'operator errors' made by doctors, physicists, programmers, ancillary medical professionals and support staff, the emphasis here is on the problems due to software glitches or programming mistakes. The software lacked proper checks and balances allowing high doses of radiation to be entered and transferred to the patient.

Modes for correcting defects will vary, but the first step is to document the problem, take screen shots of the defect, create a formal notice to alert the vendor about the defect, and immediately discontinue any related usage creating risk. In cases of security vulnerabilities, the system may need to be taken offline until the resolution of the issue.

Buying Non-Compliant Software

Your entire organization is expecting the software to meet national standards or federal mandates, but what if the vendor fails to develop their product by these guidelines? In the case of the Electronic Health Records (EHR) Incentive Programs, being disqualified becomes a possibility.[3] Moreover, penalties for non-compliance are enforceable.

[2] https://www.classactionlawsuithelp.com/radiation-overdose-class-action-lawsuit/. Accessed December 15, 2016.

[3] https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/. Accessed December 30, 2016.

Compliance Standards

Most buyers inherently assume a vendor meets compliance standards if they are on the list of the Office of National Coordinator for Health Information Technology (ONC) approved vendors. However, some vendors may have up to 5 to 10 different versions of software in their solution stack, though only certain versions meet the standards. Far worse, a certified product today may not stay certified in the future.

Therefore, we recommend that you first determine if your software meets the compliance standards by ensuring it complies with the Health Information Portability Assurance Act (HIPAA) Security Rule and HIPAA Privacy Rule. HIPAA establishes a national standard to protect health information. It outlines how to handle sensitive information for storage, transfer, and communication. Elasticity and adaptability are built in to fit healthcare organizations of various sizes and structures. The software implementation team should understand compliance regulations thoroughly to ensure the policies and procedures surrounding the use of the technologies are appropriate for the size and structure of the organization and that they comply with the Privacy and Security rules. The next step would depend on the type of software. If the solution is required to meet meaningful use (MU), which will soon become part of the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) and the Merit-based Incentive Payment System (MIPS), then these products will need to meet certification by the ONC, as well.

Common software compliance slip-ups include vendors who meet a certification one year but lose it the next, vendors who fail to meet new standards or vendors who release software that creates challenges to meet these standards. Due to stiff competition, some vendors will offer very 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 their user will comply, they will guarantee the software will meet standards, or they will pay the penalty.

Penalties for Non-Compliance

If your organization is found to be non-compliant, there can be a resolution by establishing corrective action; however, if this action is not immediately implemented, financial penalties can be assessed. In the case of HIPAA, there are two levels of penalties that can be issued: civil and criminal. Civil is applied when the individual or organization was not aware of the violation, if there was reasonable cause for the violation, or if it was willful neglect. The civil penalties can range from $100 to $50,000 per violation. Criminal penalties, being more severe, have fines that range from $50,000 and one year in prison to $250,000 and up to 10 years imprisonment.[4] In the case of meaningful use, the penalty would be a reduction in Medicare compensation. It should be noted that meaningful use participation is NOT mandatory, whereas HIPAA is required by law.

[4] Healthcare Business & Technology. http://www.healthcarebusinesstech.com/hipaa-violations/. Accessed November 30, 2016.

Not Seeing the Writing on the Wall

Technology is continually being improved and replaced by newer and better technology. When a new software is released, older programs fall out of rotation and are no longer supported. For example, say your organization implements a system that is working and meeting the needs of the organization, but your vendor has commercially discontinued the product and is no longer creating enhancements. In short, you are on a sinking ship. Not acting or refusing to accept the obvious will only delay the unavoidable reality of having to rip and replace your system.

The Writing or the Discontinued System Trap

When a vendor commercially discontinues a system, it is time to look for a new one. A discontinued system or product is like out-of-date personal technology, such as laptops and cell phones. When a vendor discontinues a product, software updates are no longer available. In the absence of these updates, the product becomes more susceptible to cyber security threats and glitches. This quandary can cause your organization to fall out of compliance, and, therefore, subject to penalty fees, as well as interruptions in the day-to-day workflow due to slow or malfunctioning software. Usually, software innovation and future features will follow regulations. For example, meaningful use stage two requires a patient portal. While your initial version may not have had a portal, this feature is now required. Now for the fun part: Does the vendor inherently provide the portal in their next release or will they expect you to pay extra for this add-on? Your contract should state that the vendor is expected to provide the necessary system functionality to stay in compliance *at no additional cost to you* since this is a mandatory feature.

What to do on a Sinking Ship

If your system has been discontinued or is nearing discontinuation, you should begin the search immediately for a more current product. Though the system will still function, and you may see no immediate changes in the day-to-day operation, your data will no longer be safe from cyber criminals. While no one enters a vendor partnership expecting to be in this situation, most are surprised to find out how little protection they have under these circumstances. Today, many systems are hosted via cloud computing. This scenario means there is a possibility that system access could be discontinued without a path forward to operate independently of the vendor and their discontinued product. Healthcare provider organizations should have a clear understanding of what to expect upon termination and/or in the event of a discontinuation of a product and, specifically, how to migrate to another solution in such an event.

One-Offs

A "one-off" is when you cave to pressure from a department or individual who needs a specific IT solution to fill in gaps around the existing solution. Although a one-off may offer some temporary relief, it will create fragmentation and eventually make it harder to evolve quickly into a more enterprise-wide ecosystem. You will also run into application retirement[5] challenges and the need to archive and store data properly for a system that may have just been used to fill a temporary gap. In some cases, you have no other option, but there can be some trapdoors in the process. It is always best to see if there is a workflow workaround or if there can be a behavior change by those who feel they must have their own solution.

Going Live with an Incomplete System

The pressure to go-live on a new system is often driven by a vendor who is trying to recognize revenue by burning through the hours in the budget so they can get to the next installation. The system, in some cases, is not properly tested before going live. As a result, the users or physicians get burned by a bad experience, and they start backsliding in the use of the application.

The Solution

This conundrum can be avoided by adopting a simple plan to Design, Build, Validate, and Test (DBVT). For example, design your order form, build your order form, validate the build with end users, and test the form with end users. This exercise will help you avoid moving forward with an incomplete system design.

Conclusion

The fatal healthcare IT decisions outlined in this paper can be avoided by modifying the agreement with the vendor during the contracting phases. For example, many vendors offer a money back guarantee if their product does not comply with the meaningful use program. Every contract should have a warranty that requires a vendor to correct defects at their expense, and under no circumstances should you sign a contract without being entitled to future upgrades and new releases. As for the "one-offs," sometimes this dilemma comes down to doing whatever the "powers that be" dictate, but the unintentional consequences of unique solutions should always be known and discussed in advance.

Contract reviews should be standard practice to ensure your organization is protected from these fatal IT decisions. These studies ideally would be conducted during the contracting phase,

[5] http://cokergroup.com/wp-content/uploads/2015/07/Options-for-Application-Retirement-in-an-Age-Where-Critical-Patient-Data-Resides-in-Legacy-Systems_September-2016.pdf

before anything is signed and agreed, although they can be completed at any time to advise an organization on how to improve their information technology.

Coker will provide a complementary contract review of existing or new solutions to provide input and guidance on how to minimize the likelihood of fatal purchasing and contracting mistakes. To have a free contract review, call Jeffery Daigrepont at 678-832-2021.