



Contact: Todd Stabelfeldt & Emily Warren  
Phone: 615.496.9607  
Email: [Emily@SolutionsByC4.com](mailto:Emily@SolutionsByC4.com)

## The Quiet Threat to Patient Data

October 27, 2016 -- In the world of pathology labs, whether in hospitals, clinics, or at independent sites, there is a quietly growing threat. It's one that ultimately threatens the patient and their health information. According to Andy Patrizio in his November, 2015, CIO Magazine online article [What end of support for SQL Server 2005 means for CIOs](#): "Compliance is as problematic for SQL Server 2005 as it is with Server 2003. HIPAA and PCI compliance both require up-to-date, patch databases, just like they do with the operating system. So if you're using SQL Server 2005 for anything related to HIPAA or PCI, you will be out of compliance [as of April 2016]." The reason this issue is such a serious threat in upcoming inspections is the fact that [as many as 800,000 servers are still using SQL Server 2005](#) as of March, 2016 – with SQL 2008 also near end of support.

There is a lot of patient data living on those SQL Servers. Fortunately, inspections are in place to protect the patient. In the laboratory, if a related issue is found, it could lead to HIPAA, CAP or other inspection fines. Prior to inspections, if shortcomings are realized as traits of a current operation, a balancing act is performed by administrators who weigh: is the magnitude of fines we may incur higher than the cost of keeping our systems up to speed?

To answer this critical business question faced by many lab directors, managers and administrators, there needs to be a frame of reference. Which can be difficult to find. There are a lot of costs associated with passing inspections in laboratories: amount of properly trained people, state of equipment and its maintenance, appropriate sample storage and management processes, the list goes on. So, how important are IT matters in comparison to all of these other concerns?

A fitting way to gauge the importance of where it ranks is through its cost to the organization. So, we conducted discussions with laboratory managers responsible for operational costs for a quick sampling which put IT expenses as the third highest cost. According to Rusty Wyles, IT Director of Pathology Consultants of New Mexico, "IT is in the top three costs as a medium average over the years. Sometimes as high as 2nd or down to 5th during years with fewer projects. IT has been staying higher with the need to implement interfaces and other projects related to government regulations." Others have similar rankings based on our sampling and IT is typically the next highest cost after labor and laboratory equipment. Yet many labs are still running a version of MS SQL Server that is over a decade old...eons in IT terms. So, there must be a common reason attention gets delayed.

The root cause of laboratories not upgrading systems and software is interoperability. The [Healthcare Information and Management Systems Society](#) defines it this way: "Interoperability describes the extent to which systems and devices can exchange data, and interpret that shared data. For two systems to be interoperable, they must be able to exchange data and subsequently present that data such that it can be understood by a user." Each software company upgrades their versions on a continuous basis and it's very common for software companies to release an upgrade once a year or more. In these upgrade paths, there are "upgrade requirements" which will routinely involve operating systems, Microsoft Server or SQL Server versions. This makes the cost of upgrading compounded at times. With this in mind, administrators oftentimes wonder why the software companies don't take on a larger role in advising on server and database matters in the process.

The reason for this is simple: there are too many IT environment variables such as related computer and server versions for them to conceivably address issues like database server upgrade needs. Software

companies do care about the state of their customer's IT environment...they would prefer they are fully compliant and high performance to make their software run optimally. But they are simply not in a position to manage these other variables for their customers out of practicality. Which puts the onus on the individual managers of each laboratory. And their budgets are constrained and they are competing against other compliance forces.



Which results in the quiet threat: systems that are out of compliance and patient data that is at risk. The costs to change the situation can be substantial. Left unattended, however, administrators not only need to ask about the likelihood of being fined for non-compliance, they also need to ask: what is the likelihood of damaging public relations and social media if we're found woefully out of compliance?

These are important questions to ask and should be asked immediately. Time is of the essence as the follow up version, SQL Server 2008, also lost mainstream support status from Microsoft in 2014 and now only has extended support available – which [expires in July of 2019](#). Consequently, the patient data risk trend is growing making the timeliness of knowing IT compliance status an even higher priority.

Fortunately, there are solutions available. IT Service companies that specialize in analysis and system implementation typically start with assessments and provide roadmaps to compliance. By following these roadmaps in an ongoing journey, administrators will know where their threats lie, what they are doing immediately to get compliant, and what they will be doing next. This is very useful information in reports to their board of directors. By asking questions and having a plan, administrators can give a loud voice to the quiet threat – and can get their own peace of mind in the process.