Newsbytes, 5/14

Raymond D. Aller, MD, and Hal Weiner

How to avoid becoming a ‘legacy system junkyard

The constant churn of information technology applications is creating new security and financial risks that health care organizations—including laboratories—must systematically address, IT experts say.

Organizational mergers, acquisitions, and the replacement of lab information systems, electronic health record systems, and other solutions often lead to a “legacy system junkyard” of little-used yet costly applications, according to Steve Davis. He is manager of enterprise archive and decommission at Dignity Health, a San Francisco-based health system with 40 hospitals in California, Arizona, and Nevada, and hundreds of outpatient clinics in 17 states.
In 2013, Davis helped lead an IT application decommissioning project at Dignity Health that resulted in the archiving, purging, or storing of 62 applications, the recovery of more than five terabytes of data, and the decommissioning of 390 servers. That has helped save the health care system $4.5 million—so far. The Dignity Health team plans to retire a total of 192 applications and sees a potential for saving nearly $10 million over five to six years.

When an application is decommissioned, it cannot simply be sent down the technology memory hole. State requirements vary, but some patient records must be kept for as long as 25 years, Davis said in a February presentation at the Healthcare Information and Management Systems Society’s annual meeting in Orlando, Fla. The CAP, meanwhile, recommends that policies for retaining patient records meet or exceed CLIA ’88 requirements. For example, the CAP says surgical pathology and cytology reports should be retained for 10 years, while forensic autopsy reports should be kept indefinitely.

But as time passes, the cost of maintaining access to all of that information adds up, Davis said. Legacy applications that are not used frequently must be housed somewhere, adding to an institution’s storage and server costs. Furthermore, in-house staff, independent contractors, or IT companies must be paid to support and maintain the system. And the older a system gets, the more difficult and costly it becomes to find someone with the knowledge to operate it. Vendors can charge as much as $1 million annually for maintenance of a current application or system and another several hundred thousand dollars annually for hardware support for a legacy system, Davis added.

Security is another downside to leaving legacy systems in place, says Jon Massey, Dignity Health’s senior director of enterprise technology services. “Over the long term, it’s riskier to just let the data sit out there. No one is paying attention to these legacy systems. There is the risk of a data breach,” Massey tells CAP TODAY. “These legacy systems, from a security perspective, are not typically integrated into your active directory or into more effective security environments.”

Despite the eye-popping savings Dignity Health’s decommissioning project has achieved so far, Massey says, it is the potential pitfalls of data insecurity—and the huge fines associated with it—that made the business case.

“The key thing we sold the project on is risk mitigation,” he says. “We’re taking these old systems that have a less secure environment and moving them to a highly encrypted, extremely secure environment that is very controlled.”

As Davis noted in his HIMSS presentation, the cost of data insecurity can be “phenomenal.” He recalled an occasion when he was about to ship 1 million records’ worth of data—properly encrypted—to Dignity Health’s data center in Phoenix through a certified courier. It occurred to him that if those records were lost and unencrypted, the firm would face $1 billion in fines, at $1,000 per patient record.

“So you can see why putting that data away and getting it away from general use . . . can be very important financially,” he said.

As critical as it may be, the legacy system retirement process is no easy task. The Dignity Health team had to do a top-to-bottom inventory to get a handle on the number of applications running, vendors associated with those applications, type of data stored, platforms used, and so on. Some functions, such as billing, required “active archiving” so the finance department could continue to collect payments and edit accounts on years-old bills. To help with this task, Dignity Health purchased a MediQuant data-transition management solution.

Many of the hospital’s other applications need mass archiving but don’t require that staff be able to read or edit the data. For these applications, Dignity Health chose an IBM product that can encrypt data and compress it by as much as 90 percent, Davis said.

The biggest challenge in the decommissioning process, he noted, was retiring old applications that lacked documentation and that had complicated and extensive data structures. Some of the hospitals acquired by Dignity Health were still using the Massachusetts General Hospital Utility Multi-Programming System, or MUMPS, first developed in the 1960s for MGH and released for the last time in 1995.

“I think there’s three people left living who can deal with MUMPS and they’re very expensive,” Davis said. Extracting the data from such systems, often written with proprietary code, can be vexing and costly. Vendors may offer to translate the data into machine-readable format—for a hefty price tag.

“One vendor quoted us $250,000 to perform the extracts, to get our own data back,” Davis said. Dignity Health eventually found a contractor to do the job for one-tenth of the price.

While the aforementioned expenses and savings apply to a big health care system, says Massey, independent laboratories and other medical groups face a similar financial scenario.

“That old system does have the risk of breach,” he says. “It could cost millions of dollars, and if you’re a small business, that could put you out of business.”

Federal report classifies health IT based on patient safety

The FDA has released a draft report in which it proposes regulating health information technology based on product functionality and potential risks to patients and not on the technology platform used.

“The safety of health IT relies not only on how a product is designed and developed, but on how it is customized, implemented, integrated, and used,” the Department of Health and Human Services stated in a press release.

The report, developed by the FDA, Office of the National Coordinator for Health Information Technology, and Federal Communications Commission, proposes three categories of health IT functionality—administrative, health management, and medical device.

The administrative health IT category includes products that pose “little or no risk to patient safety” and, therefore, require no additional oversight by the federal government, HHS reports. These include software for billing and claims processing, scheduling, and practice and inventory management.

The health management health IT category, according to HHS, contains products “of sufficiently low risk and thus, if they meet the statutory definition of a medical device, FDA does not intend to focus its oversight on them.” Regulation of these products should be provided through “ONC-coordinated activities and private sector capabilities that highlight quality management principles, industry standards, and best practices,” the agency adds. Among the products in this category are systems for provider order entry, medication management, and electronic access to clinical results, as well as most clinical decision-support software.

The medical device health IT category is a narrowly defined group of products that could pose a safety risk to patients if they do not perform properly and, therefore, should continue to be regulated by the FDA, HHS reports. This category includes computer-aided detection software, software for bedside monitor alarms, and radiation treatment software.

The draft document is an outgrowth of the Food and Drug Administration Safety and Innovation Act of 2012, which directed the FDA, ONC, and FCC to develop a risk-based regulatory framework for health IT that promotes innovation, protects patient safety, and avoids regulatory duplication.

The FDA opened a 90-day public comment period on the draft document on April 7. The three federal agencies also held a public meeting May 13–15 to solicit comments and gather feedback on the report.

SBCNE adds email report delivery to AP system

Small Business Computers of New England has introduced an add-on email report delivery module for its AP Easy anatomic pathology system. The module allows labs to securely email password-protected, encrypted PDFs of pathology reports to clients.

Reports are sent in PDF format in a Zip file. Clients have the option of password protecting the PDF report or the Zip file, or both.

Reports can be emailed automatically at sign-out to the physicians referenced on the case, or they can be emailed any time after a case is signed out to any physician in the user's physician library. Users can limit the number of reports that can be sent in each email or send reports in batches, if their email server permits. Users also have the option of sending reports to multiple email addresses.

Small Business Computers of New England, *800-647-2263*

AHIMA concerned about EHR copy-and-paste functionality

The American Health Information Management Association has issued a position statement warning about the dangers of using copy-and-paste functionality within electronic health record systems.

"Misuse of this functionality has the potential to result in or contribute to several overarching challenges, with implications for the quality and safety of patient care, medico-legal integrity of the health record, and fraud and abuse allegations," according to AHIMA.

The position statement proposes that public and private sector organizations work together to ensure appropriate use of the copy-and-paste feature and reduce potential risks.

Among its recommendations are that industry stakeholders collaborate on developing and promulgating copy-and-paste best practice standards. The standards should include alternative approaches to documentation capture, such as linking to the original source instead of duplicating the information.

The agency also recommends that the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology include appropriate copy-and-paste functionality within EHR certification criteria.

Health care provider organizations, AHIMA reports, should address the use of copy-and-paste features in their information governance processes and provide all EHR users with comprehensive training on the proper use of copy-and-paste functionality. Providers should also monitor compliance and enforce copy-and-paste policies and procedures, taking corrective action when needed.

Among the challenges and risks associated with copy-and-paste functionality, AHIMA continues, are inaccurate, outdated, or redundant information; inability to identify the author or intent of the documentation; propagation of false information; and inconsistent or unnecessarily lengthy progress notes.

NovoPath debuts Web portal

NovoPath has developed a customizable Web portal for its NovoPath anatomic pathology system to help its clients comply with federal legislation requiring labs to provide direct patient access to lab test reports. Patients can log on to the Web portal through a lab's website to download reports generated through NovoPath's AP system.

NovoPath*, 877-668-6123*

Data Innovations launches Laboratory Intelligence solution

Data Innovations is offering its new solution, Laboratory Intelligence, in the recently released version 8.13 of its Instrument Manager middleware.

Laboratory Intelligence, or Lab Intel, provides customizable dashboards, allowing access to actionable performance metrics. Key performance indicators displayed on the dashboards help quantify and measure the success of activities.

Critical analytics and drill-down capability help identify revenue and cost trends early and isolate the root causes.

Data Innovations*, 802-264-347*

[hr]

Dr. Aller is director of informatics and clinical professor in the Department of Pathology, University of Southern California, Los Angeles. He can be reached at raller@usc.edu. Hal Weiner is president of Weiner Consulting Services, LLC, Florence, Ore. He can be reached at hal@weinerconsulting.com.