

Automated Surveillance: Can it Replace "Shoe-Leather" Epidemiology?

Copyright 2009 by Virgo Publishing.
<http://www.infectioncontroltoday.com/>
By: Kelly M. Pyrek
Posted on: 07/24/2009



A recent survey of infection preventionists (IPs) by the Association for Professionals in Infection Control and Epidemiology (APIC) confirmed that while demands on the profession are escalating, 41 percent of respondents to the "2009 APIC Economic Survey" reported reductions in budgets for infection prevention in the last 18 months due primarily to the economic downturn. With resources failing to keep pace with these demands, many IPs are strapped for the funding and staff necessary to ensure that their efforts to monitor and report healthcare-acquired infections (HAIs) are optimized.

Perhaps that's one reason why in June, APIC announced its support for the use of automated surveillance technologies in the healthcare setting as an essential part of infection prevention and control activities, and published its position paper, "The Importance of Surveillance Technologies in the Prevention of Healthcare-Associated Infections."

Wright (2008) acknowledges that "Although most infection control programs have little trouble accessing data, many find themselves overwhelmed in the efforts to translate data into information and, finally, knowledge. However, if infection control programs are to transcend from regulatory requirements to change makers, our dependence on data must diminish." Wright (2008) says that medical informatics, known as "the study and application of methods to improve management of patient data ... relevant to patient care and community health," is a powerful aid for infection prevention, but warns, "In the absence of astute and committed owners (i.e., IPs), this tool remains dulled, broken or unused."

For the uninitiated, today's surveillance technologies are computerized systems designed to collect infection data quickly to help pinpoint and investigate potential clusters of HAIs in real time. They streamline a process that can be labor intensive and limited in scope when performed manually. However, many IPs resort to "shoe-leather epidemiology" because their hospitals lack the technology; in fact, APIC's economic survey showed that among respondents, just 1 in 5 had electronic data-mining technology at their fingertips.

"Recent outbreaks, like H1N1, have highlighted for hospitals the need for systems and hardwired processes that proactively identify outbreaks with potentially global ramifications," says Scott D. Pope, PharmD, national director of SafetySurveillor from Premier Inc. "Manual processes often prone to missing such trends and not facilitating rapid, ongoing evaluation of patient level data are no longer acceptable norms."

Wright (2008) says that a lack of an automated system can cripple an infection prevention program: "The absence of AS leaves the practitioner(s) to manually collect, review and transform data into knowledge. A key step in the process, review, demands excellent attention to detail and the ability to recognize patterns across time and distance. Understandably, it can be an imperfect practice. However, these limitations can, and often do, lead to missed opportunities for cluster detection."

"Unfortunately for the overworked IP, there will always be a need for "shoe-leather epidemiology," says Tracy Gustafson, MD, worldwide director of infection prevention software development and medical affairs for BD Diagnostics - Diagnostic Systems. "Both of the IP's main duties (surveillance and preventive education) require face-to-face contact with people, and no matter how sophisticated computers become, they cannot replace clinical judgment and observation. What automated technologies can do is to help the IP work smarter, by converting 'data' in existing hospital databases into 'information' that can be used to improve patient care. To accomplish this, software must behave like a responsive 'computerized assistant' that extracts and translates HAI-related data from other hospital systems, monitors prevention practices, and reduces paperwork by automating routine and/or mandatory reporting tasks. Of course, considering the daily workload of an IP, responsive end-user support and hands-on software training are essential."

Stanley L. Pestotnik, MS, RPh, president, chief executive officer, and co-founder of TheraDoc, Inc. notes, "Based on my 30 years of professional experience in clinical informatics, the single most important lesson learned is that workflow will change based on surveillance technology. An open mind, as well as training and support from the software partner, are paramount. For those who embrace the technology, computerized surveillance systems can transform the role of IPs — relieving them of the cumbersome, time-consuming task of hunting for and manually analyzing data, and freeing time for vital activities such as interventions and staff education. For example, using the TheraDoc Infection Control Assistant, Rhode Island Hospital estimated that computerized surveillance allowed its IPs to reduce the amount of time they spend at their desks reviewing microbiology and other reports by up to 50 percent. A word of caution, however — the need for good 'shoe-leather epidemiology' will not be altogether eliminated with these systems. Electronic systems will enhance and focus 'shoe-leather' investigations to allow the process to be more efficient and more quickly yield answers."

"As a vendor it would be tempting for me to say that it is easy for an IP to move from a traditional shoe-leather approach to infection prevention to automated technology...but it simply wouldn't be true," says Colin Hung, vice president of marketing and alliances at rL Solutions. "It takes effort, commitment and open minds to make this transition successfully — anyone who tells you otherwise hasn't been through it. It is hard to change the systems and processes that have been internalized for years at healthcare facilities. It's not that IPs don't want to change; on the contrary, many of the ones we have worked with are eager to lead change within their organizations — it's that the entire organization has to be willing to change. It takes more than one IP to make the transition from manual to automated — it takes whole parts of the organization, like microbiology, unit managers, physician groups, administration, and, of course, IT. Gaining and sustaining buy-in from these important stakeholders is the biggest challenge and most pressing concern for IPs." Hung continues, "In some organizations these stakeholders need to be convinced that automated infection prevention technologies

will actually make a difference. Some require ROI analysis, complex impact assessments and other such justification studies. At other organizations these stakeholders need to have a clear picture of what their worlds will be like when these automated systems are brought in."

Industry can help IPs make the transition from a manual system to an automated system less taxing.

"As vendors, one of the ways we can best help IPs is to work side by side with them to gain stakeholder buy-in," Hung says. "As an industry we can help by establishing new best practices in the use of automated infection surveillance systems, sharing benchmarking data that is standardized and accepted across the healthcare industry, collaborating to reduce the complexities of integration with healthcare IT system (interoperability) and facilitating communication between healthcare organizations who have successfully made the transition to electronic infection control systems and those who have yet to."

Charles Westergard, BSPHarm, MBA, vice president of clinical affairs for Senti7, admits, "Infection preventionists are familiar and comfortable with traditional pen, paper and spreadsheet technology. My sense from talking to many IPs is that they feel they don't have the time to learn the newer systems available — the learning curve is too steep. Vendors of these systems can help by doing excellent user-centered design to simplify interfaces so 'clutter' and alert fatigue are minimized. Setting up surveillance criteria and generating reporting from the systems should be clinician-driven and easy to understand without the need for IT staff support or a user manual."

"Entering into the switch with an open mind is a critical first step," Pope says. "The switch to automated technology takes time, energy and patience so mentally preparing for the investment and not expecting an effortless transition is important. Conversion to automated technology has proven to improve efficiency and patient safety and is the right thing to do."

Rob Moulson of CKM Healthcare advises IPs who are ready to make the leap to automated technology to follow these tips:

- Use an intuitive, user-friendly software that can be customized to the infection prevention program's needs
- Find a vendor that provides effective training, support and guidance throughout the implementation period and beyond

Gaynes et al. (1990) say the process for evaluating an automated system for surveillance involves five steps:

1. Evaluating surveillance objectives
2. Reviewing the current surveillance system for its advantages and disadvantages
3. Preparing a "wish list" of functions that an automated system should perform
4. Identifying available systems
5. Evaluating available systems

"One of the most pressing concerns of IPs is how to make an informed choice with different vendors and software offerings on the market," Moulson says. "A key is to know what your facility's primary needs are and to find a vendor who can best meet those requirements in a cost-effective manner. The service provider can help by understanding and ensuring their needs are met and exceeded as well as providing excellent initial and ongoing support. It also important that vendors continue to provide innovative solutions that keeps up with rapidly changing IPAC requirements."

"An infection surveillance system must be implemented before any features or functions can be applied by the end user," says Drew Deaton, director of operations for CareFusion MedMined services. "This effort should be resource-sparing for both hospital IT and for any clinical staff involved. A proven track record of efficient implementations complemented by hospital IT references and satisfied clinical end-users should be required of any vendor under consideration."

It's a lot to think about, but IPs and industry experts agree that recent outbreaks of infectious disease created greater awareness of the need for a better system for crunching the numbers and analyzing infection rate data."

Deaton adds, "Once implemented, the functionality of a surveillance system is only as good as the training provided. Additionally, ongoing customer service will often determine how well the technology is disseminated throughout the health system. Not all end-users adapt to new technology at the same rate. This requires that all training programs offer a customized approach that can accommodate all levels of expertise, both technical and clinical. Content experts in large-scale data processing and management, hospital epidemiology, statistical analysis, and clinical and financial outcomes should be part of any solution under consideration. These individual components, appropriately managed, should translate into scalability in customer support, and into maintenance of high levels of customer satisfaction during all stages of company growth. In the end, the success of any surveillance solution should be tied to demonstrable improvements in patient safety and financial outcomes. These improvements can only be achieved if a system can complement current infection prevention workflow while expanding the capability to recognize process breakdowns, share data with the affected clinical areas, and provide consistent feedback on prevention performance. All performance metrics must be based on objective, timely, reproducible, and accurate data that can be reliably compared across institutions in a meaningful and accurate way."

"Over the past several years, the widely publicized SARS, MRSA and C. difficile outbreaks have created a growing demand for better control and prevention of infectious diseases in healthcare settings," says Gustafson. "Consumers Union, the general public, federal and state legislators, and the Centers for Medicare and Medicaid Services (CMS) have all focused attention on hospital-associated infections. Hospital managers at every level—from the IP to the C-suite and the hospital board—now recognize that better technology resources are needed to alert staff when high-risk patients are admitted, to differentiate HAIs from community-acquired infections, to compare their HAI rates to national benchmarks and to monitor compliance and analyze the value of evidence-based practices. More recently, the influenza A(H1N1) pandemic has heightened awareness of the value of bio-surveillance systems that monitor for an influx of patients with specific signs and symptoms of infection."

"Recent events have created an opportunity for IPs to take advantage of the undivided attention of their C-suite," says Deaton. "IPs

have used this moment to educate their executive and clinical leadership on the prospects of improving patient safety through timely, accurate, and objective screening for both HAIs and community-based threats such as H1N1. Executives are recognizing the clear clinical benefits of providing their hospital epidemiology staff with better tools. At the same time, the current economic climate and new reimbursement guidelines require that any expenditure on infection prevention provide a real impact to the bottom line. The assessment of any healthcare IT application should include a request for evidence of attributable improvements in patient safety and financial outcomes at the client facility, in addition to demonstrations of available features and estimated time savings.”

“The recent publicity surrounding outbreaks of H1N1 (swine flu) as well as potential outbreaks such as H5N1 (avian flu) have definitely put the spotlight on the need to for increased vigilance with regard to infectious diseases,” observes Hung. “Although the media may have sensationalized the doomsday-like scenarios, the attention that has been brought to bear on healthcare’s role in infection prevention has been mostly helpful. It has highlighted the need for better processes, better technologies and more resources in the fight against infectious diseases. All around the world, healthcare providers are actively looking at their infection control practices and asking themselves the key questions: ‘Are we doing the best we can?’ and ‘Can we answer the epidemiological who, where and when questions?’ To answer these questions (and to begin taking the first steps to understanding and controlling an outbreak in a timely manner), healthcare providers need an accurate picture of their infection situation...and the best way to get that picture is with better systems for crunching numbers and analyzing infection related data. There is a wealth of information hidden in the everyday activities of healthcare providers and there are systems now available that can help to unlock these hidden nuggets of infection insight.”

Westergard agrees that the heightened public awareness of multi-drug resistant organisms and the spread of global infectious diseases is “causing the public to demand more accountability from already overstretched epidemiology and infection prevention professionals.” Westergard adds, “These professions routinely use outdated surveillance technology to identify patients that are at risk for or that have documented infections. They need to incorporate advanced surveillance and reporting into their daily routines, freeing up their valuable time to focus on the job of prevention and education. When they are looking at technology, it is important that the system can write a query to identify/track new types of infections ‘on the fly’ without a six-month wait for IT staff or the vendor to do the work. By then it will be too late.”

“The recent H1N1 influenza outbreak, as well as the spread of antibiotic-resistant infections such as MRSA, have reinforced in the minds of IPs and hospital epidemiologists that there is a critical need for electronic surveillance systems that allow for early detection and timely intervention,” Pestotnik says. “During the H1N1 outbreak, for example, many hospitals turned to their TheraDoc systems to generate alerts for patients entering the hospital with influenza-like symptoms or diagnoses of influenza so that they could be immediately isolated and tracked. Additional alerts allowed real-time notification of positive H1N1 lab results. Clinicians and healthcare executives also needed to monitor and analyze the scope and progression of the outbreak, and keep public health officials informed. In large outbreaks, the infection prevention staff would be quickly overwhelmed if they had to handle all of these responsibilities manually. The recent experiences demonstrate that computerized surveillance with advanced analytics is a critical tool if hospitals are to be prepared for infectious disease outbreaks.”

While every hospital’s infection prevention needs are different, Gustafson says the most pressing facility-specific needs “require finding new ways to motivate good infection control and prevention practices. These include improving handwashing, screening patients for multi-drug resistant organisms, enforcing central line insertion practices, feeding back surgeon-specific infection rate reports, studying new devices and technology that could reduce infections, and identifying local outbreaks or careless healthcare practices.” Gustafson adds, “These functions are critical to improving patient safety at the facility level, and sometimes get lost in the rhetoric about national concerns like pandemic preparedness, mandatory reporting to NHSN, or new payment regulations from CMS. Software helps by automating what can be automated, and alerting the IP when intervention and judgment may be needed. For example, admission-level or lab alerts can provide indicators of risk, or possible HAIs or infectious diseases to be investigated; surgical alerts can remind IPs when follow-ups are due; analysis tools can help IPs look at the relationship between practices and outcomes or infection rates at their facilities vs. national benchmarks or other facilities in their enterprise. Software also can save hundreds of hours for mandatory reporting. For instance, most hospitals and ambulatory surgical centers have an electronic surgical system which contains facility-specific procedure codes, surgical start and stop times, wound class and anesthesia scores. These items are pre-cursors to the data required by NHSN, but before they can be electronically transmitted to NHSN, the data must be verified, translated and transformed to meet NHSN coding requirements and ‘business rules.’ Systems like AICE automate these tasks.”

The Benefits of Electronic Surveillance

Wright (2008) notes, “Automated surveillance technologies have been warmly welcomed in infection control for several obvious reasons: time saved in reducing manual efforts, reduced error potential, enhanced surveillance capabilities, and ease of access. Infection control programs are continually faced with competing priorities and reduced or insufficient resources. Expectations of expanded surveillance and reporting, whether from internal, regulatory, or public, demand time from practitioners, often at the expense of education, observation, and behavior modification. To reverse this trend and hopefully expand the role of the IP as an agent of change within a healthcare delivery system, surveillance must absorb fewer human resources. Although most publications describing AS systems are retrospective or a before-after design, virtually all report a time-savings benefit.”

Linda R. Greene, RN, MPS, CIC, lead author of APIC’s position paper and director of infection prevention and control at Rochester General Health System, observes, “Automated surveillance eases the burden of data management for IPs and allows them to focus on the activities that protect patients, like walking rounds, observing procedures and educating healthcare personnel. In addition, it can help hospitals save money by targeting areas for tailored elimination strategies that reduce infections and excess cost.”

The APIC position paper outlines the benefits of automated surveillance:

1. Streamline and facilitate efficient review of relevant data, promoting rapid identification of sentinel events and detection of outbreaks
2. Expand and better define the scope of infection prevention activities
3. Reduce infection prevention department time spent on surveillance and clerical tasks

4. Improve response to public health issues
5. Regulatory compliance
6. Financial performance
7. Potential to enhance antibiotic stewardship programs

Gustafson says the most important benefits of a “computerized assistant” are improvements in efficiency. “Well-designed software can collect more data, analyze and react faster, and remember what needs to be done longer, than a dozen human assistants. Since the focus of infection surveillance has shifted from control to prevention, a key benefit is their ability to capture and transform data derived from various hospital computer systems to provide the IP with alerts about real-time, or time-sensitive, events. For example, alerts enable the IP to receive immediate notification of an MRSA re-admission, so that appropriate protocols can be followed to prevent spread. Alerts can identify the first positive culture for each organism, or flag possible HAIs for investigation, send reminders when a patient’s length of stay exceeds expected norms, or follow up with surgeons on post-discharge HAI diagnoses, etc. In all these ways, they help the IP manage time more effectively.”

Westergard emphasizes that the most significant benefit an infection prevention program can realize from advanced surveillance technology is increased time to focus on the actual prevention activities. “Up to 65 percent of an IP’s day can be spent just doing routine mundane surveillance and reporting,” he says. “This minimizes the opportunities for critical education, training and prevention activities as well as more advanced epidemiological research.”

“In light of the growing torrent of clinical and administrative data in healthcare today, electronic infection control systems must provide both comprehensive surveillance and advanced analytics,” Pestotnick points out. The old quality adage, ‘you manage what you measure’ is particularly true in the field. Timely surveillance, accurate detection, evidence-based intervention and meaningful, and defensible and comparable measurement are hallmarks of electronic surveillance systems that will yield returns on investment represented by increased physical surveillance capabilities, improved response times, increased compliance, reduced costs, and reduced infections, to mention a few.”

Moulson says that in addition to increasing staff productivity, facilities can improve dramatically their patient safety efforts with automated surveillance. “It enables IPs to increase their time performing other tasks, such as education and consulting that will help to further reduce HAIs, which is especially important now with the CMS decision to discontinue reimbursement for these infections.”

Hung emphasizes that an automated surveillance system can eliminate non-value-added administrative tasks such as reviewing every single lab result and every patient admission. “So ironically, the biggest benefit of a computerized system is that IPs get to spend LESS time in front of a computer,” he says. “Another key benefit of surveillance systems has nothing to do with the technology itself, but with the process required to implement it. The installation of an electronic surveillance application is the perfect time to review existing infection prevention processes (especially those around collaboration and communication) and is the best time to establish new best practices. As well, since a proper implementation involves several key healthcare departments such as lab, nursing units, IT, administration, this is a fantastic opportunity to strengthen the collaboration between these groups. Other key benefits of infection surveillance system include consistency of data collection; consistency across sites/units/IPs in infection information processes; wider and deeper surveillance with the same number of resources; quicker and better decisions on where to apply limited infection prevention resources; and improved staff retention – modern systems, chance to rethink processes, paperwork relief.”

The Limitations of Electronic Surveillance

Automated surveillance, like all types of technology in general, is not without its limitations, according to Wright (2008), who explains, “Paramount to these is the up-front cost investment and the need to obtain financial support. Although projected and proposed cost savings are commonly reported in the literature and marketing materials, Franklin’s adage of ‘a penny saved is a penny earned’ is difficult to prove and sometimes dismissed. Wisniewski et al. estimate an up-front investment of approximately 4,000 hours in development alone to construct an internal clinical data warehouse for infection control. Investment does not end once the system is in place. Technology’s only constant is constant change, and system owners (users, developers, administration) must be prepared for such change, including from a financial standpoint.”

Furuno JP, et al. (2008) state, “Economic considerations are major determinants in the decisions to implement, maintain, or discontinue computerized infection control surveillance systems in healthcare settings. These systems often require considerable initial capital investment followed by continued financial commitments for maintenance and support. Even if the use of a computerized infection control surveillance system is effective in increasing the efficiency of infection control surveillance, the financial burden necessitates economic analyses to inform decision makers on the utility of these systems. However, improved surveillance alone does not necessarily reduce infection rates or reduce associated costs. An important advantage of the computerized systems is that they can have decision support or notification features that may aid in other infection control activities related to surveillance, and those features could help to reduce the incidence of infections.”

Furuno JP, et al. (2008) say there is a paucity of information on cost data relating to automated surveillance in the medical literature, and emphasize, “Considerably more data are necessary to evaluate whether automated infection control surveillance is both effective and cost-effective. All future studies of these tools should attempt to assess whether increased accuracy or efficiency of surveillance methods actually impacts patient outcomes. In addition, studies should also include the collection of economic data. Again, these data should include costs and time associated with equipment (e.g., computer hardware), software, installation, staffing and education of staff, validation, maintenance, and upkeep. Previous estimates of costs of infections can be used, but this will vary among hospitals. Sensitivity analyses can be useful in providing ranges of costs and effectiveness and insights into cost-effectiveness under a variety of circumstances, and, thus, their use is encouraged.” The researchers add further, “At present, a business case for implementation cannot be based on evidence that enhanced surveillance is cost-saving from a hospital or societal perspective. However, even if sufficient evidence supporting the cost-effectiveness of computerized surveillance becomes available in the future, continued evaluation is necessary because of inherent differences between systems, differences in populations, and differences in implementation. Thus,

hospitals will still be required to complete individual business-case analyses to justify adoption of specific systems at their institution.”

Wright (2008) is quick to add that throwing money at a problem does not ensure success: “Even the most advanced systems are unable to control the most likely source of system failure -- people. Failure can come from a variety of non-technical angles including projects not meeting user requirements or expectations (often because of a lack of involving users in development), lack of planning, and ineffective communication between users and developers. Learning curves of AS systems vary, as does the knowledge and comfort level of the user.”

Wright (2008) points to a 1994 study of 8,380 information technology projects in which nearly one-third were assessed to be complete failures, and only 16.2 percent were fully successful. This resulted in a projected financial loss of \$140 billion. The leading success factors included user involvement and executive support, whereas the most commonly reported failure characteristics were lack of user input and poorly defined or changing system requirements. The most recent report from the same group showed marked improvement. Of 13,522 projects, a full one-third succeeded, whereas 15 percent failed according to the 2003 report. This further underscores the need for effective planning including early IP involvement and clearly defined work flows during system development. In addition, there remain underlying technical issues with the potential to provoke even the most advanced AS systems. Without consistent quality source data from within the institution, systems may fall prey to the aphorism GIGO (garbage-in, garbage-out). Similarly, changes to internal data structures or sources, ranging from a complete overhaul to changing a microbiology susceptibility panel, can lead to erroneous results. Although many AS systems are able to detect these aberrations, these events demand ongoing time and resources. It is especially important that the end users not become lackadaisical with the systems themselves but maintain vigilance and not assume that technology is a substitute for the critical-thinking IP.”

The Future of Surveillance

Why stop at mere surveillance, asks Wright (2008), when technology could also assist clinicians with decision-making and even predicting risk for MDROs on admission. Technology could take common risk factors such as history of colonization, previous hospitalization and antimicrobial use, and use data to predict and adjust over time. “If the flow of information between an institution's health care information infrastructure and AS systems becomes bidirectional, these models could be deployed to issue standing orders for surveillance cultures of high-risk patients to the admitting physician,” Wright (2008) notes. “Similarly, orders written for contact, droplet, and airborne isolation could be sent out automatically the moment the result is entered in the clinical laboratory, reducing the delay and decreasing the potential for cross transmission. Future developments are on the horizon, and IPs should actively participate in the process to voice their wishes for tomorrow and hopefully guide future enhancements ... Perhaps the lasting legacy of surveillance technology will be its ability to ease the burden of data management from the IP to go forth and accomplish the profession's highest calling: prevention.”

References:

APIC. The Importance of Surveillance Technologies in the Prevention of Healthcare-Associated Infections. Accessible at: http://www.apic.org/Content/NavigationMenu/GovernmentAdvocacy/PublicPolicyLibrary/Surveillance_Technologies_position_paper_2009-5_29_09.pdf

Wright MO. Automated surveillance and infection control: Toward a better tomorrow. *Am J Infect Control*. Vol. 36, No. 3, Supplement, Pages S1-S6. April 2008.

Gaynes R, Friedman C, Copeland TA, Thiele GH. Methodology to evaluate a computer-based system for surveillance of hospital-acquired infections. *Am J Infect Control*. 1990;18:40-46.

Furuno JP, Schweizer ML, McGregor JC, Perencevich EN. Economics of infection control surveillance technology: Cost-effective or just cost? *Am J Infect Control*. Vol. 36, No. 3, Supplement, Pages S12-S17. April 2008.

Surveillance Roundtable With Industry Experts

ICT asked industry experts to address key questions relating to the implementation of automated surveillance systems.

ICT: What are the most critical components of a computerized infection control surveillance system?

Gustafson: “Most critical to the success of any computerized system is how well it communicates with the IP, and how well it enhances workflow. A good system will automate tasks that computers do well, freeing the IP to do higher level tasks while providing more timely data for real-time intervention. And since healthcare technology is constantly changing, users need to be able to modify their system to reflect changes over time. An infection surveillance and prevention solution should provide data that help the clinician determine when an HAI might be present, but not make the final decision for the clinician. These determinations now affect CMS reimbursement, state legal mandates, and the validity of NHSN data used for benchmarking, so it would be unwise to allow computers to have the final say. In that regard, the system should allow the IP to make manual edits to the data (e.g., to indicate when a positive culture is not associated with an HAI). It also should provide the ability to compare hospital outcomes to national benchmarks, or to internal norms where national benchmarks are not available or appropriate. Finally, many IPs will tell you that mandatory reporting of HAIs, MDROs and reportable diseases takes an inordinate amount of their time. So, a critical component is to help IPs identify and report HAIs easily. These are all capabilities that AICE provides.”

Moulson: “There are several: Rapid and flexible infection surveillance and reporting capabilities to save time; integration with external systems to further reduce the time to create cases, retrieve information and facilitate data mining; time-saving outbreak management that also improves patient safety by providing early warnings of potential outbreaks; and powerful infection analysis that can provide a wide range of statistical, graphical and analytic reports.”

Pestotnik: “The most critical element is interoperability to ensure the seamless exchange of data between different hospital computer systems and ensure that data elements are correctly understood by the system despite variations in terminology and coding. Systems

also must capture data from a variety of hospital sources, including ADT (admission, discharge, transfer), lab, pharmacy, microbiology, radiology, and surgery, to ensure accurate reporting and data analysis. Finally, enhanced, simplified workflows should include integrated views of coherent, useful information that empower and focus the attention of the user on critical patient safety issues. IPs also should understand terminology such as "real time," which is not well defined among system vendors. Some systems batch results and report them periodically throughout the day, but true real-time information provides the best opportunity for intervention. For example, batch reporting may delay notification of MRSA results, preventing the opportunity for immediate isolation and risking the spread of infection. IPs understand their clinical needs but may not be experts in information technology and terminology. In light of the proliferation of surveillance technologies, asking the right questions will help them evaluate the options and make the best decisions for their hospitals' current and future needs."

Pope: "The position paper published by APIC appropriately highlights the essentials: aggregating clinical data from multiple systems into a single source, retrieving data in real-time, translating data into useful information and sending electronic messages to agencies such as the National Healthcare Safety Network (NHSN)."

Westergard: "The implementation and setup time, maintenance and IT resources needed are key concerns that don't get much attention. The power that comes from an easy-to-use system cannot be underestimated. A good surveillance system supports IPs' efforts, it doesn't replace them. Time to setup and manage the system should be minimal and not require the support of IT staff. Maintenance of an on-site server can be problematic and require additional overhead to manage, maintain and upgrade the system. Web-based, hosted models eliminate these issues. Access to the system is easy and upgrades and maintenance are the vendor's issues to work through."

ICT: How can infection preventionists best demonstrate ROI of a computerized infection control surveillance system?

Deaton: "Delivering an ROI for any surveillance system is dependent upon the infection prevention team sharing objective, timely data with both the front-line clinical staff and the C-suite. But frequent communication with the executive team on financial outcomes and analysis may not be part of infection prevention's current responsibilities. However, the work of infection prevention and surveillance still represents a significant impact to the bottom line. In order to implement this approach, a surveillance solution must offer the capability to objectively recognize HAI reduction opportunities at the unit level, as well as housewide. The IP may then act as a facilitator, communicating performance data to the bedside staff and outcomes data to the executive team."

Gustafson: "We have already discussed the many benefits of a computerized infection control system. However, converting these benefits to dollars and cents is not easy. Cost avoidance methods (summing the extra treatments and length of stay related to an HAI) are tricky, because you can't prove how many infections were prevented or preventable. However, CDC has published reasonable estimates of the attributable cost of infections, and the percentage that are preventable, and these annual totals easily outweigh the cost of AICE. Furthermore, good software will reduce the need for clerical help, improve IP efficiency, reduce patient suffering, and can even reduce isolation costs. Decision-makers shouldn't overlook the marketing value and other intangible benefits of a modern infection control system. Patients are looking for hospitals that put patient safety first---that make every possible effort to shorten hospital stay, avoid unnecessary complications, and minimize patient suffering."

Hung: "Sadly, the best way to demonstrate ROI does not yet definitively exist – proof that electronic systems can reduce the rate of infections within a healthcare facility. There is a mountain of anecdotal evidence, but as yet there is not a defining study that has proven this to the level where the entire industry has accepted it. It is, however, only a matter of time before this happens. Until then, if an organization is in the process of or thinking about evaluating a computerized infection control system, then the best way to demonstrate the potential ROI of a computerized system is to answer two key questions: How much time does it take us today to do find patients who potentially have infections (i.e., surveillance) and to produce reports for the various stakeholders? and What other important tasks could we be doing if we didn't have to spend so much time on question 1? If an organization has already made the investment in an computerized infection control surveillance system here are some of the ways an IP can demonstrate ROI:

- Keep metrics from before and after the project like infection rates and time studies on how IPs spend their day
- Use the system to present reports whenever and wherever possible (resist the temptation to use MS Word or Excel)
- Use the system daily to set the example for the organization
- Track the cost savings of detecting infections early"

Moulson: "To help quantify time savings, an IP can compare how long it takes to perform certain tasks with and without using a computerized infection control surveillance system. For example, one of our clients reported an average reduction of over 15 minutes to document a case when using the IPAC Administrator. When taking into consideration that this facility has on average 1,000 cases a year, this translated into over 250 hours of time savings. Other areas to quantify include improved patient safety through the detection of potential outbreaks and receiving timely alerts such as when a patient with a communicable disease is admitted or readmitted to a facility."

Pestotnik: "ROI should be assessed in a number of ways, including:

- Timeliness of surveillance activities compared with the manual system
 - Earlier identification of issues
 - Earlier intervention
- Physical breadth of surveillance activities—are you able to do more with the same FTEs?
- Increased available time for prevention and education

- Compliance rates to required activities and reports
- Infection and reimbursement rates

Numerous ROI examples exist for infection control surveillance systems. For example:

- The Mayo Clinic in Jacksonville, Fla., presented data at the 2004 SHEA conference showing that the TheraDoc system helped the hospital prevent five to six infection-related deaths per year and achieve annual antibiotic drug cost savings equivalent to the annual license fees for the surveillance technology.
- TheraDoc surveillance technology was part of a multi-pronged approach used by the Hospital of the University of Pennsylvania to achieve a sustained reduction in central line-associated bloodstream infections of more than 90 percent over three years. University clinicians said the findings, which were presented at the 2009 SHEA meeting, "provide a road map for cutting the deadly, costly toll of healthcare-acquired infections nationwide."

Pope: "Consider a comprehensive picture when identifying savings. There are efficiencies that can drive infection rates down, resulting in shorter lengths of stay and reduced cost of care. These efficiencies can also equate to existing staff doing the work of more people (i.e. three IPs being able to do the work of four) which relate to very tangible FTE savings. From these larger amounts all the way down to quantifying the reduced paper utilization can demonstrate savings and contribute to green initiatives hospital wide."

Westergard: "ROI can be demonstrated in one of two ways. The first is in brand awareness. Publicly-reported infection rates affect the brand (and thus the revenue) of the hospital. The use of advanced surveillance can leverage an IP's time to focus more efforts on prevention rather than detection. These prevention efforts should ultimately lead to lower infection rates and a better brand awareness in the public's eye. Secondly, IPs need to work with their partners in pharmacy to assist and guide in antimicrobial stewardship efforts. Effective pharmacy-driven antimicrobial stewardship programs have shown real reductions in drug budget and reductions in resistance rates. Identifying a surveillance product that supports infection control and their pharmacy partners yields a larger ROI than using a product that focuses on infection prevention alone."