SCOTTSDALE INSTITUTE

information edge

May 2007
Volume 13, Number 4

Business Continuity Comes Home

EXECUTIVE SUMMARY

If you think redundancy is something healthcare needs less of, you're only half right. That's a correct assumption when discussing duplicate laboratory tests and other redundant exams, of course. However, there's another kind of redundancy—redundant or backup IT systems—that healthcare organizations need more of and which helps them maintain business continuity in the face of unplanned interruptions. Given the huge investment healthcare is making in automation and the recent confluence of natural and manmade disasters, terrorism, pandemic threats, HIPAA and other regulatory factors, business continuity has become an imperative for the healthcare CEO.

Business continuity planning or BCP—sometimes put under the umbrella of business continuity management—encompasses the people and processes that must be recovered or maintained in the event of a disaster in order for a hospital or health system to continue its core operations of patient care. For example, BCP focuses on ensuring that departments like radiology continue to function during a catastrophe. Disaster recovery (DR), a subset of business continuity management, refers specifically to IT recovery. BCP and DR must be integrated, but typically have different owners, says David Sarabacha, a Portland, Ore.-based senior manager at Deloitte & Touche LLP (Deloitte & Touche), who is certified as a professional continuity manager by both the DRI International and Business Continuity Institute.

In this issue of *IE* we seek to share best practices in healthcare BCP and DR by talking to executives at Deloitte & Touche as well as at leading integrated delivery systems like Saint Luke's Health System in Kansas City, Intermountain Healthcare in Salt Lake City and Johns Hopkins in Baltimore. Besides its bottom-line objective of ensuring the continuity of mission-critical care, we found that an unforeseen benefit of BCP is the enhanced communication and understanding that is generated between IT and business units. For SI members, that's always been a win-win.

SCOTTSDALE INSTITUTE

Membership Services Office:
1660 Highway 100 South
Suite 306
Minneapolis, MN 55416
T. 952.545.5880
F. 952.545.6116
E. scottsdale@scottsdaleinstitute.org
W. scottsdaleinstitute.org

WELCOME NEW SPONSOR

Deloitte.

The Scottsdale Institute is proud to announce Deloitte Consulting LLP as a Sponsoring Partner.

Deloitte Consulting brings together over 60 years of proven industry experience with the innovation and knowledge of nearly 2,500 professionals who deliver a complete range of audit, tax, consulting, and financial advisory services across all sectors of the life sciences & health care industry. Deloitte offers comprehensive, customized solutions that can help health care providers maximize opportunities and master their most pressing and complex challenges.

As part of their overall healthcare professional service offerings, Deloitte provides specialized consulting expertise in strategy and operations, and the application of information technology to integrated delivery networks and large academic hospitals.

Welcome Andrew Vaz, National Managing Principal, Mitch Morris, MD, Principal, and the rest of the Deloitte team.

Interest spikes

Sarabacha has helped hospitals do business continuity planning for nearly 15 years and witnessed how the current wave began in the late 1990s when hospitals made a big push in IT-based disaster recovery planning. Interest spiked in early 2000 with Y2K and 9/11, expanding the focus to all business and patient care processes. "We're continuing down that path. With an escalating number and geographic dispersion of natural disasters combined with an ever increasing reliance on application systems for critical data, BCP has never been as hot a topic as it is now. We're seeing entity-wide plans that include emergency response at the front end, move through crisis management on to business continuity and disaster recovery planning," he says.

David Sarabacha, senior manager, Deloitte, Portland, Ore.

Deloitte.

"It's coming down to having an EMR—you can't be manual anymore. There really is no more paper backup to go to," says Sarabacha, who defines business continuity management as the umbrella under which hospitals and health systems can create a four-part internal management structure: *1) Emergency response*—Actions in the first few hours, including for example, human-safety issues like determining the number of private ambulances available; *2) Crisis management*—Communications/PR, what an organization decides to say both internally and to the media; *3) Business continuity*—Process recovery; *4) Disaster recovery*—Supporting IT, including network infrastructure and applications.

"There are varying interpretations, but it really all comes under the rubric of risk management, including a general requirement under HIPAA, within any good governance structure," he says. "It's not unlike Sarbanes Oxley. Business continuity is not required explicitly but clearly must be part of any comprehensive risk-management strategy."

Codependencies

Fiona Williams, a partner in Deloitte & Touche LLP's Southern California office focused on enterprise risk services in life sciences and healthcare, says dependency on IT has skyrocketed as more and more healthcare environments have become automated, exacerbated by the burgeoning number of interfaces with laboratories, providers and "smart" biomedical devices.

Fiona Williams, partner, Deloitte, Los Angeles

And doctors who have gotten used to having their data available have little patience with system downtime. "They get upset if the system is down for even an hour. It's become more visible. In the past disaster recovery was just a back-office issue to them, but not anymore," she says.

This type of dependence was starkly obvious in the business world recently when the operating system for the Blackberry PDA crashed and left many users desperate to reconnect with what they consider their communications lifeblood. Sarabacha says that event underscores the increasing reliance in IT on third parties. The discipline of business continuity management tries to tackle that challenge by rigorously identifying and securing all third-party IT sources, in the process asking key questions such as: Am I reliant on lab results from a single vendor? Am I reliant upon a single electric utility provider or do I have a single power feed into the facility regardless of multiple providers? "It is absolutely critical to do a single point of failure and vulnerability analysis as well as a financial and operational impact analysis, to focus an organization's resources appropriately when planning. The objective is to first mitigate your operational risks and then develop cost-effective recovery solutions for the remaining risk," he says.

Cost of doing business

While hesitant to quote exact figures because each situation is unique, Sarabacha warns hospitals they must be prepared to make significant capital outlays for business continuity, essentially duplicating much of their existing hardware for backup purposes and hiring specialized personnel. "You may have to replicate your entire [system] in order to be able to get EMRs up immediately, then another set of software applications two to three hours later. There are buckets of recovery time involved and all of those are getting pushed closer as the organization's reliance on IT increases," he says.

Williams asserts that one of the biggest obstacles to successful BCP is industry denial. Many hospitals and health systems have yet to "get it" in terms of grasping the underlying risk and costs associated with an outage. "What organizations don't do is include that calculation in the system development life cycle. As you roll out a system it should be embedded as part of the initial cost. What happens instead is that we're dependent on special funding requests," she says.

"When you go through the process of acquiring software, part of that initial cost should include security and business continuity. That doesn't occur in most environments, so you end up saying we need to look at funding—and it's a hard sell to get that funding. It doesn't fall into the IT organization; it's viewed as an extra. It's an afterthought. We'll deal with that later, and then later never happens," Williams says.

Some IT departments allocate partial funding for BCP and DR. "You'll see 30% to 50% of the budget for backup, but then you don't know if it's for 30% to 50% of users or 100%. They give you a little bit of money, but the result is that you're in limbo," she says.

Mix of solutions

Traditionally, industry and healthcare have contracted with vendors such as

WELCOME NEW SPONSOR

NAVIGANT CONSULTING

The Scottsdale Institute is proud to announce Navigant Consulting, Inc. (NCI) as a Sponsoring Partner.

Navigant Consulting, Inc. (NYSE: NCI) is a specialized independent consulting firm providing litigation, financial, healthcare, energy and operational consulting services to government agencies, legal counsel and large companies facing the challenges of uncertainty, risk, distress and significant change. The Company focuses on industries undergoing substantial regulatory or structural change and on the issues driving these transformations.

Navigant Consulting has a proven reputation in achieving long-term results for hospitals, health systems and other healthcare providers regarding operations improvement, strategic planning, and interim management. Services include revenue cycle solutions, clinical documentation improvement, coding, financial advisory, clinical operations improvement, supply chain management, and information technology strategy.

Welcome Steve Heck, Rick Skinner, and the rest of the NCI team.

For information on any of these teleconferences, please register on our Website scottsdaleinstitute.org

June 13
KLAS on Ambulatory EMRs in Large Physician Practices
- Jared Peterson, KLAS Enterprises, Orem, Utah

June 18
Race to Results: Accelerating Knowledge Adoption to Improve Quality at CHCA
- Donna Payne, EVP, Child Health Corporation of America, Shawnee Mission, Kan.
- Janet Guptil, consultant, Health Evolutions, St. Louis, Mo.

June 21
The Coyote Crisis Campaign: A Successful Regional Crisis Response Solution in Arizona
- James Cramer, CIO, Scottsdale Healthcare, Scottsdale, Ariz.

June 26
Integrating e-ICU and Robotics at Parkview
- Susan Ahrens, MD, director, Adult Critical Care, Parkview Health, Fort Wayne, Ind.

July 10
KLAS on Smart Infusion Pumps
- KLAS Enterprises, Orem, Utah

July 11
NYU Medical Center's CPOE Big Bang: Success Factors and Lessons Learned
- Pravene Nath, MD, assistant professor, School of Medicine and Senior Director, Information Technology, NYU

more events on next page

SunGard to provide backup data centers called "hot sites" typically hundreds of miles away. However, the current trend is to eschew such outsourcing and instead bring it in-house, partly because during 9/11 air transport was grounded, making it impossible for staff to reach the hot site. "Most people don't want to leave their families in a regionalized disaster to go halfway across the country. The current recommendation is to locate alternate processing sites no less than fifty to sixty miles from the primary location, so it is close enough to commute; it allows you to get there by car, but protects against a more regionalized disaster event" says Sarabacha. Still, not everybody is following the advice. Some organizations continue to contract with data centers in locations such as Colorado or Arizona because there appears to be fewer geographically-based risks in those areas and it's less expensive to do business.

Creative solutions abound, depending on speed-to-recovery requirements and the ability to "load balance" by having two sites running simultaneously. Recovery can be nearly instantaneous in such scenarios, he says. "You can do a hybrid and increase performance. It's easier to defend from a business perspective."

It's also a strategy that should appeal to health systems that find themselves with new data centers as a result of acquisitions. Instead of shutting them down and eliminating staff, health systems can use those otherwise duplicate facilities as internal hot sites to back up critical applications.

Given the increasing options on the market, hospitals should use due diligence. Some IT firms provide hospital data-center services via an ASP (application service provider) model in which all the hardware is outsourced. Sarabacha cautions that these arrangements typically do not provide DR for systems. Such contracts may stipulate that the vendor will use "best efforts" in recovery, but that does not imply any legal obligation to provide DR. "It's mostly ala carte. You typically have to pay for recovery separately," he says.

If funding for BCP and DR is a problem, Sarabacha suggests healthcare organizations leverage the funding available for pandemic or avian-flu planning. "Now that you have that funding, use it as a stepping stone to build continuity plans for other risk events," he says.

Bringing recovery home

A year ago, Saint Luke's Health System recruited Theresa Crawford as information services disaster recovery manager to bring recovery capability in-house.

Theresa Crawford, DR Manager, Saint Luke's Health System, Kansas City, Mo.

Saint Luke's Health System
saintlukeshealthsystem.org

"We needed to demonstrate the ability to recover our most mission-critical clinical applications locally," she says, "because when you contract with a third party for DR, the resources

to achieve this can be hundreds of miles away. When you contract with an outsider they typically provide 48 hours turnaround minimum. If you do it locally you can recover without any interruption at all." Still, Saint Luke's has not ruled out vendors altogether, reserving them for financial applications like payroll processing.

Saint Luke's determines which applications to bring in-house for recovery by prioritizing them in seven tiers: 0 through 4 are to be recovered locally; 5 through 7 will rely on a vendor. Zero denotes no downtime whatsoever; 1 must be recovered within 30 minutes or less; 2 in two hours; 3 in four hours; 4 in 12 hours; 5 in 24 hours; and 6 must be brought back within 48 hours.

Saint Luke's has designated one of its existing facilities as a permanent backup data center, raising the floor and adding a large training room for support staff. The 15,000 square-foot site, whose renovation will be complete in 2008, is only 25 miles from Saint Luke's Hospital. "The ideal distance," says Crawford, whose dual role includes data-center manager.

The People v. IT

"DR is part of business continuity," she says, "but because I'm in IT the focus is on DR, which involves tasks like making sure the phone trees are working. DR focuses on the IT part. BC is the people aspect of it—plans & procedures, processes and practices. It includes relocating staff, even if they are to work from home."

The organization conducted its first test in April using a temporary backup facility, cutting recovery time to only six hours from a previous 24 to 36 hours. "Our first attempt was very successful," says Crawford, partly because the staff was experienced in the overall recovery process. The biggest change was that they did not have to travel. Future tests are scheduled twice a year.

"Everybody in the healthcare industry seems to be trying to establish local recovery," says Crawford, who has extensive DR experience, mostly with financial systems. "Lots of companies leverage existing facilities. As an added bonus you can save a lot of money by utilizing that facility for isolated disasters like a localized fire, for example. You have workstations, telephones, servers, different types of drives and modems."

BCPWHO?

As president of the Business Continuity Planning Workgroup for Healthcare Organizations (BCPWHO) and manager of data security and disaster recovery at both Johns Hopkins Hospital and Johns Hopkins University in Baltimore, Bill Rider has as broad a perspective as anyone as to what's happening with business continuity across the country.

"We're seeing an interesting evolution. A lot of different components of risk management are converging," he says. Those components include: 1) The relationship between IT disaster recovery planning and hospital disaster management, including

Upcoming Events continued

July 16
IT Cost Benchmarking: Creating Apples to Apples Peer Comparisons
- Patrick O'Hare, senior VP and CIO, Spectrum Health, Grand Rapids, Mich.
- Derek Mazurek, project manager, Spectrum Health

July 18
Software Quality – A New Reality
- Kent Gale, president, KLAS Enterprises, Orem, Utah
- Tim Zoph, CIO, Northwestern Memorial Hospital, Chicago

July 19
IT Cost Benchmarking: Creating Apples to Apples Peer Comparisons
- Patrick O'Hare, senior VP and CIO, Spectrum Health, Grand Rapids, Mich.
- Derek Mazurek, project manager, Spectrum Health

July 23
New York City Gives EMR's to Medicaid Providers
- Farzad Mostashari, MD, assistant City Health Commissioner

July 30
Medication Administration Rounding at Partners HealthCare
- Anne Bane, RN, MSN, Nursing Professional Development, Partners HealthCare System, Boston
- Thomas Cooley, assistant pharmacy director

For information on any of these teleconferences, please register on our Website scottsdaleinstitute.org

Kudos to CEO IT Achievement Award winners

Modern Healthcare and HIMSS announced their 2007 CEO IT Achievement Award winners and they are all Scottsdale Institute members! Congratulations to Alan Aviles, president & CEO, New York City Health and Hospitals Corp; John Ferguson, president and CEO, Hackensack University Medical Center; and Michael Murphy, president & CEO, Sharp HealthCare.

Alan Aviles

John Ferguson

Michael Murphy

Bill Rider, DR Manager, Johns Hopkins Hospital and University, Baltimore

surge capacity in a disaster; 2) Business-capacity planning, including downtime procedures and workarounds; 3) University crisis-management planning—If there's a campus-wide emergency event, how do we alert students? "A variety of forces are causing this convergence including natural and man-made disasters, and regulatory compliance. In our hospital environment, patient care and patient safety are paramount, and the IT systems support that patient care focus," he says.

"Should I try to put an umbrella over all these components to my risk? We see a lot of organizations facing this question. This trend is not limited to healthcare," says Rider, who joined cohorts at other academic medical centers to form BCPWHO [www.bcpwho.org] as a go-to resource for sharing lessons learned and best practices in business continuity.

On foot in the IT jungle

But it's his work at Johns Hopkins, where he has dealt with a widely heterogeneous landscape of IT platforms and applications and varied operations for more than seven years, that he has learned the most. "We range across the board from the very large, centralized mainframe environment to very small Intel-based open systems." Actual systems range from student application systems to sophisticated clinical applications within an EMR as well as payroll and benefits.

Rider is getting to know it all up close and personal.

"A lot of the work we're doing focuses on documenting and analyzing," he says, profiling the applications according to hardware, software, network and recovery-time requirements, and identifying key people—done via assiduous data collection and personal interviews. Rider estimates the process covers 60 to 75 core applications, with one-hour interviews of each key staffer, up to three people per application.

"We find out exactly when the customer absolutely has to have a particular application back up. Then we put them into a logical sequence within a larger strategy. I can then begin to construct actual recovery timeframes and provide those to our customers. I'm trying to understand customers' expectations and build a strategy that will try to meet those expectations," he says.

Think about not having IT

Johns Hopkins already has an overall recovery strategy which it tests twice a year and it tests many applications individually. But that's an old-world approach that's increasingly insufficient. "As the next iteration of this whole BCP effort, we're trying to definitively document what the recovery sequence will be in a unified way, taking into account multiple platforms in

multiple IT environments, utilizing both external (vendor) solutions and internal resources," Rider says.

This in-depth BCP dialogue has proven to have multiple benefits, for both IT and business operations, including giving IT the ability to explain to the customer issues like loss of IT service. "It forces them into a thought process about the impact of not having the system," says Rider. "They see how IT and operations go hand in hand."

It's greatly improved from the old way of communicating with business units. "For years, IT would sit down with customers and throw a lot of acronyms at them, and actually run the risk of alienating them. If you go to a customer with quantified recovery time objectives and explain what makes up that metric, then the customer can understand—and they can come back to IT and say: If you're telling me 24 hours, that's too long. IT can then respond with alternatives and costs. If it's two hours, let's negotiate impact of downtime versus cost of recovery. The business units and IT are negotiating to strike that optimum recovery point," Rider says.

"You definitely want to go through face-to-face interviews. It's important to give the customer a chance to provide the business perspective. And as an IT person I need to really understand what their issues are. It's good "IT good will" to shake hands and meet the people," he says. Still, the informal communication should be combined with documentation templates that are easily incorporated into the DRP/BCP software Johns Hopkins uses.

Shadow governance

Karl West, associate VP for Information Services at Salt Lake City-based Intermountain Healthcare, presented an SI teleconference entitled "Intermountain Healthcare: Documented and Tested I.S. Disaster Recovery Process and Procedures" on May 8. [The audio presentation and slides are available to members on the SI website. Click on "Teleconferences" in the left column under "Members Only."] West says one of the most critical elements in DR is creation of a governance structure. Intermountain started at the bottom by first creating the role of data security administrator.

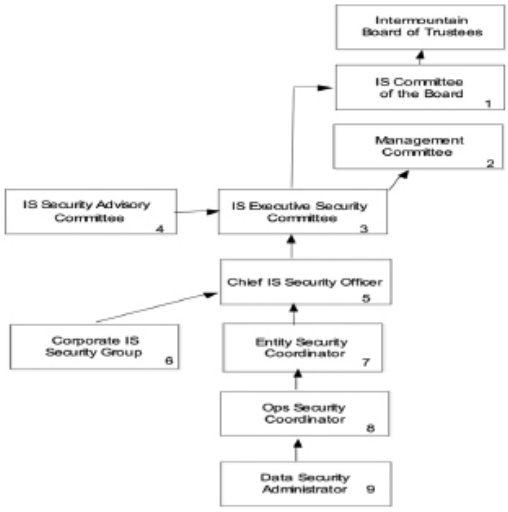
IHC INTERMOUNTAIN HEALTH CARE

"We have a large number of hospitals and clinics and 2,600 applications. Each application is administered day to day by someone at the facility," he says. For example, a designated radiology staffer is responsible for administrative responsibilities for the PACS (picture archiving and communication systems, the digital imaging system) like adding or deleting users. "What we've done is brought that person into the security model. That hadn't existed in the past," says West.

The data security administrator in turn reports to an operational security coordinator who is the director of IS operations

"You definitely want to go through face-to-face interviews. It's important to give the customer a chance to provide the business perspective. And as an IT person I need to really understand what their issues are."

at a hospital. [see chart below] That person reports to the Entity Security Coordinator, a hospital business person who reports to the chief IS security officer (West's title). A corporate IS security group also reports to West and provides design and oversight of the health system's security. It meets with him bi-weekly to advise on everything from how people are hired to what disaster plans are in place.



Intermountain's IT security structure.

Matrix of criticality

West sits on the IS executive security advisory committee, a six-person group that oversees his role that includes legal counsel and the CMO. It sets security strategy for the entire organization. There's also an IS security advisory committee of 25 people—including CFOs and COOs from across the health system—that helps the executive committee prioritize business needs.

Intermountain's objective is a DR structure and plan that's completely integrated with clinical and business processes and IS and is annually updated with clinical, business and IS input. If the governance structure is the chassis, the engine for this entire effort is the IS Criticality Matrix tool, a large database that prioritizes the top 100 of the organization's 2,600 applications and identifies their critical functions and associated dependencies. It's reviewed and tested annually using "Mock Tabletop" exercises planned by the CSO and facilitated by the corporate IS security group.

West oversees an IS DR master plan that describes processes and procedures, emergency communication information and definitions. It also contains IS system and application composition, dependencies, general recovery steps, IS and business-owner contact information, vendor information and other relevant details. "We're trying to get away from an IS-directed process to one that is business-directed," he says.

The underlying assumption to any plan is that disasters will occur and that the goal is to mitigate risk as much as possible.

Conclusion

The explosion of interest in business continuity planning and disaster recovery in healthcare reflects the industry's dependence on IT, growing interdependence among providers and other healthcare players and the maturing of overall risk management. It's no longer justifiable to treat BCP as a nice-to-have—because for provider organizations the term business continuity also means patient-care continuity.

If the governance structure is the chassis, the engine for this entire effort is the IS Criticality Matrix tool, a large database that prioritizes the top 100 of the organization's 2,600 applications and identifies their critical functions and associated dependencies.

Top executives at leading integrated delivery systems like Saint Luke's, Johns Hopkins, Intermountain and many other SI members have come to this realization.

"It's imperative we have well thought-through and well-planned disaster recovery," says Marc Probst, CIO at Intermountain, who recalls a vivid lesson in just how valuable DR planning can be. "We completely lost our data center two years ago when a metal washer from a static switch for our electrical system converted itself into a 38-caliber bullet and shot around [inside the system]. The switch was the single point of failure and we lost the data center, but because Karl and his organization had planned so well our most critical applications—HELP2—were available in just three and a half hours. All applications were fully back up in eight," he says. "He saved my bacon."

Marc Probst, CIO, Intermountain Healthcare, Salt Lake City

Scottsdale Institute Conferences 2007/09

Fall Conference 2007
Hosted by Piedmont Healthcare
Sept. 27-28, 2007
The Ritz-Carlton, Buckhead
Atlanta

Spring Conference 2008
April 16-18, 2008
Camelback Inn,
Scottsdale, Ariz.

Fall Conference 2008
Hosted by Northwestern Memorial Hospital
Sept. 25-26, 2008
Chicago

Spring Conference 2009
April 29-May 1, 2009
Camelback Inn,
Scottsdale, Ariz.

SCOTTSDALE INSTITUTE MEMBER ORGANIZATIONS

Advocate Health Care, Oak Brook, IL

Allina Hospitals & Clinics, Minneapolis, MN

Ascension Health, St. Louis, MO

Billings Clinic, Billings, MT

Catholic Healthcare West, San Francisco, CA

Catholic Health Initiatives, Denver, CO

Cedars-Sinai Health System, Los Angeles, CA

Charleston Area Medical Center, Charleston, WV

Children's Hospital of Pittsburgh, PA

Children's Hospitals & Clinics, Minneapolis, MN

CHRISTUS Health, Irving, TX

Cincinnati Children's Hospital Medical Center, Cincinnati, OH

DeKalb Medical Center, Decatur, GA

Hackensack University Medical Center, Hackensack, NJ

HealthEast, St. Paul, MN

Heartland Health, St. Joseph, MO

Integris Health, Oklahoma City, OK

Intermountain Healthcare, Salt Lake City, UT

Legacy Health System, Portland, OR

Memorial Health System, Springfield, IL

Memorial Hermann Healthcare System, Houston, TX

Munson Healthcare, Traverse City, MI

New York City Health & Hospitals Corporation, New York, NY

New York Presbyterian Healthcare System, New York, NY

North Memorial Health Care, Minneapolis, MN

Northwestern Memorial Healthcare, Chicago, IL

Norton Healthcare, Louisville, KY

Parkview Health, Ft. Wayne, IN

Partners HealthCare System, Inc., Boston, MA

Piedmont Healthcare, Atlanta, GA

Provena Health, Mokena, IL

Rush University Medical Center, Chicago, IL

Saint Luke's Health System, Kansas City, MO

Saint Raphael Healthcare System, New Haven, CT

Scottsdale Healthcare, Scottsdale, AZ

Sentara Healthcare, Norfolk, VA

Sharp HealthCare, San Diego, CA

Sparrow Health, Lansing, MI

Spectrum Health, Grand Rapids, MI

SSM Health Care, St. Louis, MO

Sutter Health, Sacramento, CA

Texas Health Resources, Arlington, TX

Trinity Health, Novi, MI

Truman Medical Center, Kansas City, MO

University of California Los Angeles Medical Center, Los Angeles, CA

University of Chicago Hospitals & Clinics, Chicago, IL

University of Missouri Healthcare, Columbia, MO

SCOTTSDALE INSTITUTE SPONSORING PARTNERS