CHAPTER 5

# ERM in Practice at the University of California Health System

GRACE CRICKETTE
Senior Vice President and Chief Risk and Compliance Officer, AAA Northern
California, Nevada, and Utah; former Chief Risk Officer, University of California

T he University of California's Health System is comprised of numerous clini-
cal operations, including five medical centers that support the clinical teach-
ing programs of the university's medical and health sciences schools and
handle more than three million patient visits each year. The medical centers pro-
vide a full range of health care services in their communities and are sites for the
development and testing of new diagnostic and therapeutic techniques. Collec-
tively, these centers comprise one of the largest health care systems in the world.
    The University of California Office of the President's Office of Risk Services is
responsible for developing and implementing enterprise risk management (ERM)
systemwide, identifying and developing strategies to minimize the impact of risk,
developing a center of excellence for managing risk, reducing costs, and improving
safety by executing new ideas and strategic plans in a rapid manner in support of
the university's mission of teaching, research, public service, and patient care.

## THE ENTERPRISE RISK MANAGEMENT PROGRAM

The University of California (UC) System began an ERM initiative as a natural
progression of making the decision to adopt the Committee of Sponsoring Organi-
zations (COSO) Internal Control—Integrated Framework in 1995, and in that same
year UC's vice chancellors for business and finance accepted an internal audit rec-
ommendation to adopt COSO as the Internal Control Integrated Framework for the
university. In 2004, COSO's inclusion of enterprise risk management into its model
led to the hiring of a chief risk officer (CRO) tasked with implanting enterprise risk
management.
    The chief risk officer, who had previously implemented ERM for a publicly
traded company, set out to learn about the operations and culture of the university
and identify what ERM activities were already in place and where there were gaps,
and what would be the best approach for implementing ERM. Visits were made

to all of the campuses and medical centers, and leaders from various departments and disciplines were gathered together and asked: *How do you know if you are doing well? What data do you have to let you know how you are doing?* Leadership clearly was able to articulate their objectives and the risks that could impact those objectives, but the data for measuring and monitoring were not timely and were primarily ad hoc, annual, and manual. The information gathered through these meetings was critical for understanding and developing the key performance indicators (KPIs) that would later become an important component of the ERM program. (See What Is a KPI?)

## What Is a KPI?

Generally, strategic or operating plans will identify the critical success factors and key goals of an organization. Critical success factors are the areas that the organization must focus on and do well in to satisfy customer/client needs. An example may be "meeting client expectations." KPIs are derived from critical success factors and define these critical success factors into more meaningful criteria. For example, the critical success factor of "improve productivity" might have KPIs such as cost, service quality, cycle time, streamlining of processes, and reduced duplication and/or rework.

### How often can KPIs be updated?

KPIs can be updated as frequently as the data they are drawn from is updated. Some examples:
Claims information, daily
Payroll information, monthly
Construction scheduling, quarterly

### How is improvement measured with KPIs?

Improvement is measured by looking at ratios between time periods relative to risk. For example, in the area of workers' compensation:

Recordable rate = Number of injuries relative to the hours worked

Next, an ERM panel was formed to develop an ERM strategy. The ERM panel included management representatives from the Office of the President, the campuses, and the health system. The CRO along with the ERM panel recognized that, given the complexity of the university's operations and the general decentralization of services and information, technology would need to be leveraged to identify, manage, and monitor risks. The overall strategy was to develop a data warehouse that could manage information already being collected by various groups, existing programs, and initiatives throughout the system—an enterprise risk management information system (ERMIS). Once consolidated in a single

location, the data could then be used to analyze processes, risks, and controls systemwide.

As the ERMIS was being developed, the CRO commissioned a cost of risk study to be able to measure and monitor success of the ERM program. The first Risk Summit was held with more than 100 attendees, and the charge was given to the attendees to reduce the cost of risk by 16 percent in 24 months. How? At the summit the program Be Smart about Safety (BSAS) was launched, which was the first of many initiatives focused on preventing and managing risk. The university not only met this charge, but exceeded it by meeting the target in only 18 months.

## Leveraging Technology to Support ERM

UC continues to develop the ERM information system (ERMIS), a flexible and dynamic system, to give campus stakeholders at multiple levels the information they need to make business decisions in a timely and effective manner. The ERMIS essentially "democratizes" information, in that it has the ability to provide key data and reports to personnel at all levels and locations of the university. As the data integrated has become richer and its use more widespread, the value of the ERMIS has grown in creative ways.

The ERMIS started with simple risk assessment tools and expanded to include:

- Dashboard reporting on major areas of risk
- Control and accountability tracking platform
- Risk mitigation and monitoring tools
- Survey capabilities

All of these tools can be used independently or interdependently, allowing for:

- Better quantitative analysis capabilities
- Improved analytical and reporting capabilities
- Support for leading risk governance and compliance processes
- Systemwide visibility, with local flexibility
- Scalability without additional burden on UC staff

While the ERMIS dashboard system is prepopulated with some KPIs, UC continues to work with each location to develop KPIs that are helpful to supporting the location's own initiatives. ERM groups find the ERMIS to be an important tool for identifying and understanding risks. The system will also support the monitoring of internal controls and accountability, providing valuable information to the controllers and internal auditors. These capabilities lower the overall cost of risk (oftentimes associated with day-to-day operations) across the institution.

The creation of automated reports within the ERMIS increases workforce efficiency. Redundancy is reduced by the creation of automated reports made readily available to those with a need to know. Instead of having the same or similar reports being developed and maintained without the benefit of shared knowledge at different divisions, departments, schools, campuses, medical centers, and other
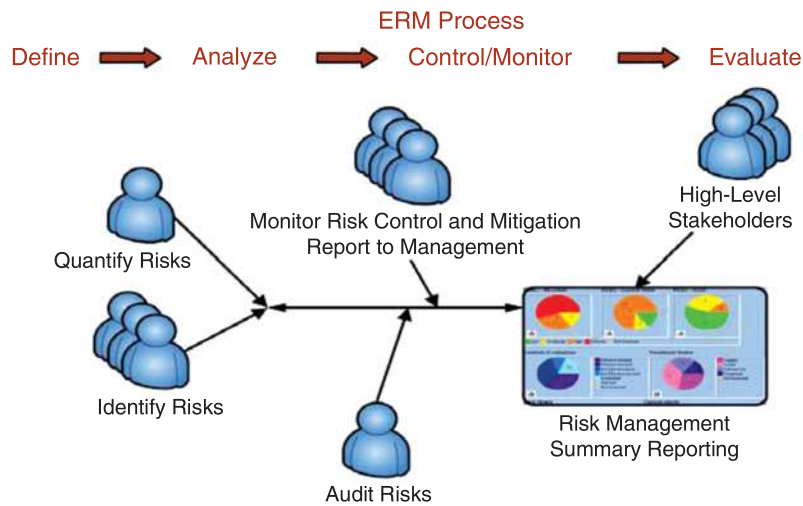
**Exhibit 5.1**   ERM Process

locations, the ERMIS enables sharing of analyses and information easily and efficiently across multiple different locations. (See Exhibits 5.1 and 5.2.)

## Creating a Risk-Aware Culture

The foundation of the University of California's enterprise risk management program is to have people actively manage their various risks—everyone is a risk manager! One key to creating a culture where everyone is a risk manager is to give them tools that meet their specific needs. That means developing different tools, work groups, and initiatives, but delivering them in a cohesive and integrated manner. Also, how can we create personal ownership for identifying, managing, and monitoring risk? A group of forward-thinking people at UC Davis came up with a solution, and the My Managed Risk portal was born!

The My Managed Risk (MMR) portal was designed as an entry point to the services and resources provided by the Office of Risk Services. It serves as a centralized location for authorized users to access enterprise risk management–related tools and information. The portal allows users direct access to their authorized ERM applications, as well as the ability to view content related to the ERM Solution Set, and at the same time to stay informed of up-to-date news and articles directly related to enterprise risk management. The streamlined design also provides an efficient way for users to search within the MMR portal in order to retrieve contents of interest quickly. (See Exhibit 5.3.)

## Health System Specialized Programs

The UC Health System participates in and benefits from all of the tools and programs that come under the umbrella of ERM, but, in keeping with delivering the right tools to the right people, UC continues to develop programs specific to health care.

**Exhibit 5.2**   ERMIS Dashboard Samples

| Dashboard Name | Description |
|---|---|
| CFO Division AIM: Actionable Information for Managers | Promote positive administrative behavior at the campus level via campus-by-campus comparisons. Results are indicative of business/operational performance and are within Chancellor's realm of control. |
| Financial Accounting | Count of hand-postings, direct deposits, electronic W-2 and payments, CFR reports, and percentage of transaction not cleared. |
| Financial Services and Controls | Connexxus participation, travel spend, and savings. Purchase card expenditures, administrative efficiency, and incentives. |
| Procurement Services | Systemwide procurement savings, procurement spend under management, and percentage of transactions processed electronically by location. |
| External Finance, UC Bond Debt | Provides visibility and trending on UC bond debt by location. |
| Medical Quality | Extends medical quality reporting data to support risk management activities. |
| Travel Incidents, Calls, Claims | To correlate and report data from all travel insurance and travel agencies for UC students and staff traveling throughout the United States and world (anticipated). |
| UCSF PD Early Warning System Report | Provides UCSF PD leadership the ability to track and identify patterns of multiple staff complaints/investigations/incidents. |
| UC Travel Dashboard— Connexxus | Tracks campus adoption of the Connexxus travel system and actual savings for campuses that utilize Connexxus. |
| Waste Diversion | Contains results of the annual waste diversion campus survey. Allows for comparison of recycling/waste diversion between campuses. |
| Human Capital Dashboard | Provides human resources–related correlations by department and reason description by utilizing enrollment, FTEs, head count, hours, EPL claims, employee separation/retirement, OSHA rates, and harassment prevention training. |
| Safety Index Dashboard | Provides safety-related loss and exposure correlations by department and cause description by utilizing the following elements: WC claims, FTEs, hours, head count, vehicles, GL, student population, acres, property losses, and OSHA rates. |
| Safety Index ROI Enhancements | Illustrates the direct and indirect costs of safety risks at UC locations and enterprise-wide. |
| UC Ready | Provides mission (business) continuity plan completion counts for all locations at the department level. |
| UC Ready Department-Level Enhancements | Systemwide continuity plan completion and activity metrics at department level. |
| Reputational Risk (CDPH) | Provides aggregated counts and trends for medical center–related complaints and penalties as reported by California Department of Public Health. |
| Reputational Risk (OSHA Cube) | Allows visibility in OSHA claims against UC locations that may cause reputational risk to UC. |
| Office of General Counsel (OGC) | Provides visibility to legal cost by locations. |
| Medical Center | Provides Medical Center loss and exposure trends and correlations. |
| Medical Center PL Cube | Provides users the ability to create ad hoc reports utilizing selected Medical Center claims data. |
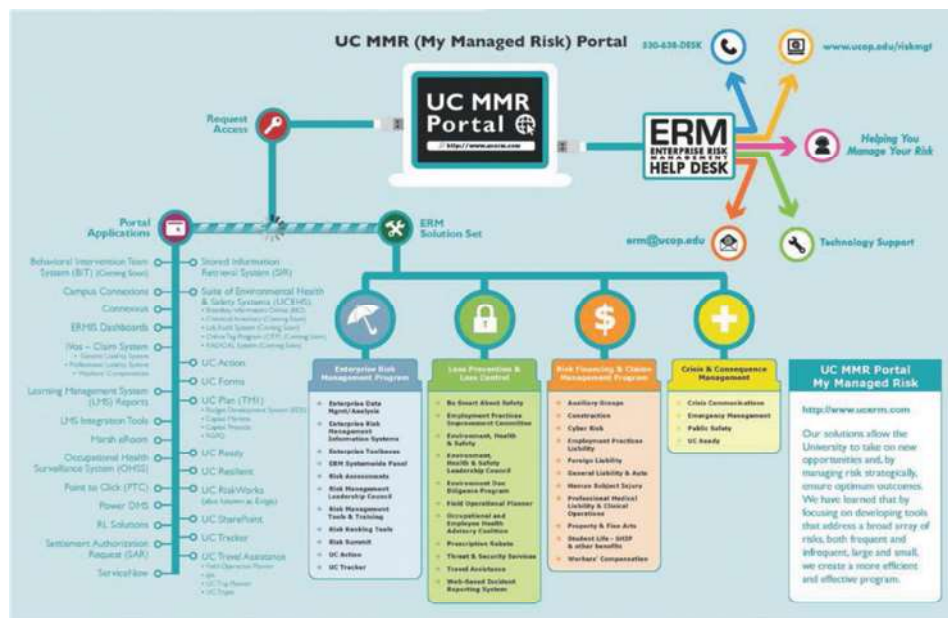
**Exhibit 5.3** UC My Managed Risk Portal

*Integrating Traditional Risk Management into ERM*
Are traditional risk management and ERM two separate programs, concepts, and disciplines? The short answer is "No." Rather, the traditional risk management practices are critical components that make up the ERM portfolio. To get at the big enterprise picture for incidents, events, and claims arising out of the medical centers and hospitals, UC developed an approach to the evaluation of medical incidents, events, and claims. (See Exhibit 5.4.)

Trending, monitoring, and reporting of adverse clinical events and their root cause(s) are done as part of ERM:

- Each University of California Medical Center uses a web-based clinical incident reporting system that permits any staff member to report an event or near miss. The university medical centers are moving to a commercial incident reporting platform that will be consistent across all facilities and permit comparison reporting.
- Each of the UC medical centers has individuals (category managers) who are responsible for the monitoring and evaluation of certain types of events and taking action on them. The Office of Risk Services has access to this system and receives notice of significant events through the system.
- Trend reports are prepared for facility patient safety and quality committees and forwarded through the facility committee structure to the facility governing body—typically the dean of the School of Medicine.
- Adverse event incidents are monitored, and serious events that may require reporting to the state are reviewed weekly; any that are sentinel events result in a root cause analysis.

| Incident (Includes Near Misses) | Adverse Event | Claim/Lawsuit |
| --- | --- | --- |
| Incident reporting system captures identified event or near miss | Adverse Event directed to Category Manager/ Quality & Risk* | Directed to Local Risk Manager, Claims Adjuster, OGC and OPRS |
| Directed to Category Manager | Serious Events identifed and reviewed by weekly Quality of Care Steering Committee | Case reviewed by facility Risk Committee for quality of care issues |
| Trend Reports developed by location Quality or Risk | Sentinel Event/Root Cause Analysis | Corrective Action is reported to Board of Regents as part of request for settlement |
| Metrics & Benchmarks | Metrics & Benchmarks | Retrospective Reviews/UC Action |
| Trend reports provided to Location Quality & Safety Committee | Trend reports provided to location Quality & Safety Committee | |
| Trend reports are forwarded to the location Executive Committee of the Medical Staff | Trends reports are forwarded to the location Executive Committee of the Medical Staff | |
| Trend Reports provided to Governing Body | Trend reports provided to Governing Body | |

**Exhibit 5.4**   UC's Enterprise Risk Management Approach to the Evaluation of Incidents, Events, and Claims

*Serious events are identified and reported to location Quality of Care Steering Committee for review. This committee is multidisciplinary and includes key individuals of the Quality & Safety Committee (e.g., the chief medical officer, other physician staff members, the chief nursing officer, legal, quality, risk, and compliance).

- In addition, the medical centers measure and review data on a number of metrics from patient complaints to infection rates, patient falls, and so on.
- Hospital-level data is compared with national benchmarks, United Healthcare (UHC) data, and so on.

Individual adverse events may result in claims and lawsuits:

- Risk Services manages the Third Party Claims Administrator to ensure that the claims are promptly investigated and appropriately resolved. As part of this process, Risk Services monitors the Third Party Administrator (TPA) performance against developed performance expectations.
- Risk Services in conjunction with the Office of General Counsel (OGC) and medical center risk management staff collaborate to ensure that the cases are well managed throughout the claims and litigation process. A select panel of defense attorneys is assigned cases.
- Risk Services through Legalbill monitors law firm billing compliance with university guidelines to ensure that the university benefits from a cost-efficient and cost-effective legal defense.

- Medical Staff Risk Management Committee at each facility reviews claims and lawsuits and makes evaluations regarding the quality of care and corrective action that is needed internally; the committee monitors the action through to resolution by the responsible departments. The Risk Services director attends the committee meetings at the locations periodically.
- There are also facilities (allocation committees) that review settled claims and lawsuits and attribute responsibility to individual practitioners or to system issues. If individuals are identified as responsible, they are reported to the external state licensing boards. Risk Services and OGC are responsible to ensure that cases are appropriately reported to both the state licensing boards and the federal National Practitioner Data Bank, and work with the locations to advise them on reporting. Both the Risk Services director and an OGC representative participate with a facility medical director to review the reporting recommendations of the local facility.
- If cases result in costs to the university, inclusive of defense and indemnity, each location has to identify the risk issues involved and the corrective action taken or planned; this action is reviewed by the Risk Services professional liability (PL) program director and the CRO; for cases of certain value, the actions are also reviewed by the senior vice president for health sciences and service.
- Additionally, the General Counsel and the Board of Regents review the corrective action that is reported.
- In addition, Risk Services has developed and implemented a monitoring system to ensure that corrective actions on cases costing the university more than $50,000 are tracked through resolution through the UC Action process. UC Action is a software tool that permits the capture of events, the causes of loss, and the corrective action that was implemented across the UC System. It permits the assignment of controls to ensure that loss prevention actions are implemented and monitored to avoid recurrence of identified issues. Developed in conjunction with UC Davis, this tool supports the Risk Services and campus loss prevention efforts. All Risk Services program managers periodically review and assess the actions being taken for appropriateness.

The role and activities of UC's Risk Services in adverse event clinical audit (quality assurance) include the following:

- The Risk Services director for professional liability manages the systemwide incident report (IR) system and receives reports of certain types of events via e-mail as well as being able to evaluate trend reports.
- The Risk Services director periodically provides reports of individual events and trends to the facility chief medical directors at their systemwide meetings. In addition, each medical director typically brings events to discuss to these meetings so that locations can learn from each other.
- In addition to the IR system, the Risk Services director is often called by the facility risk managers and alerted to serious events. The Risk Services director also serves as a resource for questions from the facilities.
- The Risk Services PL director implemented a program to ensure that all of the university's claims and lawsuits are coded for loss prevention and

trended. This was accomplished through using the Controlled Risk Insurance Company (CRICO[1]) Comprehensive Risk Intelligence Tool (CRIT). This program permits the university to identify the areas of greatest frequency and cost and the underlying contributing factors in a reliable manner. The university facilities have access to the system and are able to compare their trends against the other UC system and non-UC entities.

- The Risk Services director hosts monthly conference calls with medical center risk management staff to discuss matters of interest and loss prevention opportunities.
- Risk Services funds loss prevention activities for the medical centers and student health facilities targeted at reducing university liability. Examples include the prescription rebate program, which provided grant funds for loss prevention activities; ELM Exchange,[2] which provides online risk education; EMMI Solutions information consent program, which helps ensure patient understanding of their clinical options to improve satisfaction; the Vanderbilt Patient Advocacy Reporting System (PARS) to identify and assist physicians who are outliers in terms of patient complaints; disclosure education; and operating room technology aimed at reducing retained foreign bodies.
- In addition, the senior vice president for health sciences and services collects and reviews data from multiple sources regarding hospital performance in clinical areas other than adverse clinical events.
- UC Action summary reports regarding corrective action are shared with the Regents on high-dollar-value litigated cases in the form of reports from the Office of General Counsel.

## PREMIUM REBATE PROGRAM

In addition to the tools developed to assess risk and report on KPIs, the Office of the President's Office of Risk Services has developed programs to reduce the frequency and severity of loss. For the Medical and Hospital Liability Program, Risk Services developed a Premium Rebate Program in 2006–2012 that was known as the Professional Liability Prescription Program (PLPP), designed to encourage risk reduction initiatives aimed at reducing the cost of risk for the hospitals and schools of medicine. The program encouraged clinical loss prevention and patient safety and rewarded hospitals and medical groups for developing and implementing specific initiatives. PLPP is a good example of propagating the concept that *everyone is a risk manager*. It put loss control in the hands of individuals responsible for the outcomes. It gave them the financial resources and incentives to make a difference. There were several parts to the PLPP (see Exhibit 5.5).

The University of California (UC) Professional Medical and Hospital Liability Program (PL) is the second largest component of UC's cost of risk. In 2012, the Chief Risk Officer believed there was a need for more ERM focus on the university's five medical centers and began exploring ways to make this happen.

University of California Center for Health Quality and Innovation (CHQI) had established a system to encourage initiatives designed to create a culture of improvement with the support of the CHQI board, comprised of the five academic medical center CEOs, the six deans of the Schools of Medicine, and chaired by

## Exhibit 5.5  Professional Liability Prescription Program (PLPP)

### Grant Funds for Locally Developed Loss Prevention Initiative—Maximum Rebate 2 Percent of Premium

Requests for the 2 percent grant funds may be made at any time during the fiscal year; however, locations are encouraged to submit early.

Medical Center Risk Management offices are expected to coordinate the applications. Each project submitted for the grant funds must have both School of Medicine and a Medical Center approval if applicable. Multiple requests per site are permitted until the 2 percent is exhausted. Once the funding application is approved by Risk Services, the funds will be transferred to the campus account. The campus must transfer to the appropriate local code. The funds must be used for the approved project; failure to apply the funds to the project will result in recoupment of the funds by Risk Services. Projects will be monitored by Risk Services.

### Medical Center and School Departments Allocation of Premium—Maximum Rebate 4 Percent of Premium

Allocation of premium based on loss experience and exposure is a critical underpinning of a successful loss prevention program. To qualify for this rebate, each School of Medicine and Medical Center must implement allocation to departments using the Bickmore approved methodology. Half of the premium will go to School of Medicine for its allocation to departments and half will go to Medical Centers for allocation of premium among its departments.

Criteria:

Ensuring the location organization structure for premium allocation is current and appropriate.

Reviewing and categorizing all historical and current malpractice cases to location identified Schools and Medical Centers and then to departments and divisions within each, entering the data into the Sedgwick CMS claims system on a continuous basis.

Selecting and applying an allocation model from Bickmore recommendations to the fiscal year 2011–2012 budget.

A written report, signed by the Dean and CEO of the Medical Center attesting to the methodology employed and the amounts paid by the various departments, is required.

### Adoption and Implementation of EMMI—Maximum Rebate 2 Percent of Premium

Qualification for this rebate will require adoption and substantial implementation of EMMI by the individual locations during fiscal year 2011–2012. The

amount of the rebate will be dependent on the degree of adoption of use as measured by EMMI data.

**Use of Technology to Prevent Retained Surgical Sponges—Maximum Rebate 2 Percent of Premium**

Human error in the counting process is a significant cause of retained sponges. Technical solutions such as Surgicount provide a reliable method to assure a valid sponge count. Reducing retained sponges through reliable technology contributes to improved patient safety, enhances hospital reputation, and avoids regulatory and legal expenses.

the University's Senior Vice President of Health Sciences & Services, with a small coordinating staff based at the UC Office of the President, Oakland.

# ERM AND THE CENTER FOR HEALTH QUALITY AND INNOVATION

In January 2013, the chief risk officer for the University of California and the executive director for the UC Center for Health Quality and Innovation (CHQI) announced a new joint venture. The new joint venture—the Center for Health Quality and Innovation Quality Enterprise Risk Management (CHQIQERM)—will award up to $8 million in grants for projects designed to reduce the risk of clinical harm to UC surgery patients in three priority areas:

1. Development of enterprise risk management (ERM) within the Schools of Medicine and medical centers. This includes projects that are aimed at clinical improvements involving multiple departments and divisions.
2. Projects aimed at reducing medical malpractice claims. These projects should take into consideration issues creating the highest frequency and severity of malpractice claims within the university facilities. Claims data identifying these areas of exposure will be provided. Projects will be evaluated based on transferability and sustainability. Ability to demonstrate a return on investment will also be considered.
3. Projects aimed at improving patient safety, quality, and efficiency within the University of California medical centers.

The joint venture seeks to fund projects by UC Health faculty and staff that use an evidence-based, systems approach to minimize the risk of clinical harm to UC patients. UC's actuary will continue to evaluate the return on investment (ROI) of the projects and include evaluation of these loss prevention efforts in its actuarial study as it has in the past.

Funding is available to UC faculty and staff intending to engage in performance improvement activities at UC-owned and UC-operated medical centers. Individual projects are capped at $250,000 per academic medical center site. A five-campus project may be awarded up to $1.25 million.

"We're thrilled to partner with Risk Services," said Terry Leach, executive director of the UC Center for Health Quality and Innovation. "This collaboration will help leverage the talent of UC Health's faculty and staff to improve patient safety at UC medical centers."[3]

After an initial campus review, top-scored selections will receive a second round of review by the CHQIQERM Risk Advisory Committee in conjunction with the CHQI Operations Committee, with final selection by the CHQI board. Five-campus multisite proposals will automatically advance to receive a review by CHQIQERM.

The CHQIQERM will provide selected Project performance improvements (PIs), within three months of approval, a schedule to present their projects to various multicampus groups responsible for quality improvement and/or reduction of patient harm throughout UC, including the CHQI Operations Committee, the chief medical officer (CMO) and chief nursing officer (CNO) group, the UC quality officers, infection control officers, pharmacy chairs, CEOs, and so on. Presentations are designed to provide individuals responsible for integration of performance improvement projects throughout UC the opportunity to learn more about the funded projects, and to provide consultation for design modification, as appropriate, to increase support and acceptance of the funded projects.

By January 1, 2014, if project funds remain or if Risk Services provides additional resources, CHQIQERM will disseminate a second round of requests for proposals (RFPs), and will provide review and management pursuant to the previous year's round of funding, with projects to be completed by June 30, 2015, unless a project continuation agreement has been negotiated and agreed upon by all parties, including the CHQI board.

## PROTECTED HEALTH INFORMATION VALUE ESTIMATOR (PHIve)

The chief risk officer was invited to serve on an American National Standards Institute (ANSI) work group. The goal of the work group was to develop and publish a guide to bring attention to the risks associated with personal health information (PHI). When hospitals and medical centers perform risk assessments, they often fail to consider the magnitude of the disruption and reputational damage from a loss of personal health information.

Following participation in the work group, UC asked Bickmore (www.bickmore.net) to develop an electronic software tool for the Protected Health Information Value Estimator (PHIve). The methodology used in PHIve is described in greater detail with examples in the American National Standards Institute (ANSI) publication, "The Financial Impact of Breached Protected Health Information." ANSI's publication is available at the ANSI website.[4]

The PHIve applies a practical methodology for protected personal health information to calculate the potential (or actual) cost of a data breach to their organization. The purpose of this exciting new tool is to help PHI protectors understand the financial impact of a PHI breach so they can evaluate and recommend the appropriate investments necessary to mitigate the risk of a data breach. This helps reduce potential financial exposure while strengthening the organization's reputation as a protector of the PHI entrusted to its care.

The tool will not make decisions for you, but it will help you organize your thinking as you consider the enterprise risk management implications of a breach of protected health information.

The five steps in PHIve are:

1. Assess risks.

    Assess the risks, vulnerabilities, and applicable safeguards for each PHI home. A PHI home is any organizational function or space (administrative, physical, or technical) and/or any application, network, database, or system (electronic) that creates, maintains, stores, transmits, or disposes of ePHI or PHI.

2. Security readiness score.

    Determine a security readiness score for each PHI home by determining the likelihood of a data breach based on the security readiness score scale.

3. Determine relevance.

    For each PHI home that has an unacceptable security readiness score, examine the relevance (i.e., likelihood or applicability) of a particular cost category, and apply a relevance factor from a provided hierarchy.

4. Determine potential repercussions.

    Relevance and consequences combined create the potential repercussions of a breach. Consequences are calculated using multiple aspects of a potential breach based on a variety of considerations for your organization. Types of repercussions include reputational (loss of patients, current customers, new customers, strategic partners, or staff), financial (including costs for remediation, communication, changes to insurance, changing associates, and business distraction), legal and regulatory, operational, and clinical.

5. Total the impacts: Add up all adjusted costs to determine the total adjusted cost of a data breach to the organization.

Relevance and consequences combined create the potential repercussions of a breach. Consequences are calculated using multiple aspects of a potential breach based on a variety of considerations for your organization.

## Reputational Repercussions

Reputational repercussions of a breach may include:

- Loss of patients
- Loss of current customers
- Loss of new customers
- Loss of strategic partners
- Loss of staff (separate from staff lost due to potential disciplinary action related to a breach)

The impact of a breach may have greater reputational repercussions if it is shared through social media or other means that raise further awareness of the breach.

The demographics of those affected by a breach also change its reputational impact. Income and age are considerations for health privacy sensitivity, among other factors.

## Financial Repercussions

Financial repercussions are grouped into five segments, each of which may contain multiple types of financial costs.

1. Cost of remediation may include:
   - Investigation or forensic costs
   - Corrective action plan costs
   - Workforce sanction costs
   - Identity theft monitoring costs
2. Costs of communication may include:
   - Notifying affected individuals
   - Notifying media outlets and notifying governmental agencies
   - Public relations costs
   - Investor relations
3. Costs of changes to insurance may include:
   - Broker costs
   - Presenting and negotiating with agencies
   - Increased cost of coverage
4. Costs of changing associates may include:
   - Due diligence for new vendors
   - Transitions to new vendors
   - Increased costs of new vendors
5. Costs of business distraction may include:
   - Lost productivity
   - Opportunity costs
   - Diversion of resources

## Legal and Regulatory Repercussions

Legal and regulatory repercussions of a breach can be grouped into four areas:

1. Costs associated with actions by the U.S. Department of Health and Human Services' Office for Civil Rights (OCR), including:
   - Fines and penalties
   - Costs of additional corrective action plans
2. State fines and penalties
3. Lawsuit costs, including:
   - Legal costs
   - Settlement costs
   - Additional payments to affected individuals
   - Insurance deductibles
4. Costs associated with potential loss of accreditation or reinstatement of accreditation

## Operational Repercussions

- Incremental cost of new hires
- Costs of recruiting and training new hires
- Costs associated with reorganization following a breach

## Clinical Repercussions

- Fraudulent claims processed
- Delayed or inaccurate diagnoses
- Bad data in search results

## Total the Impacts

Add up all adjusted costs to determine the total adjusted cost of a data breach to the organization.

The pilot PHIve tool was previewed by UC's medical risk managers for the first time at the University of California's 2013 Risk Summit. Bickmore is demonstrating the tool and seeking comments from the UC medical risk managers before the tool is released. The tool was demonstrated and comments were sought from the UC medical risk managers before the tool was released.

## ERM and Strategy

Risk is an inherent and essential part of any organization. When properly managed, risk drives growth and opportunity. If enterprise risk management (ERM) is the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital, earnings, and operations, then it only makes sense that ERM is seen as a strategic tool for management.

The past several years have been a financially challenging time for the university. Even in the face of those challenges, however, the university has made significant strides in reducing its risk exposure, thereby allowing the campuses to focus their limited dollars on the university's mission of teaching, research, and service. ERM is seen in the university as a continuous improvement process and has been integrated into its Working Smarter initiative.[5]

The Office of Risk Services, as part of the CFO division, has integrated the Division Strategic Goals[6] into our operations:

- Reexamine the day-to-day
- Showcase our value-add
- Engage with the customer
- Develop our staff
- Be action-oriented

The Office of Risk Services continues to reexamine the day-to-day operations, looking for innovative ways to reduce risk while improving operational efficiency. It continues to showcase the savings that are generated by implementing ERM, and

continually engages its customers to learn how it can better meet their needs. It not only focuses on developing its staff, but encourages the professional development of those at the campuses and medical centers by providing the Risk Summit and monthly webinars. Finally, the tools and information provided by Risk Services allow campus and medical center leadership to be action-oriented and to be able to implement quickly programs that will result in immediate impacts. The guiding principle in all of the work that Risk Services does is to support the university mission of teaching, research, and public service, as well as patient care.

## QUESTIONS

1. Your Medical Group wants to expand by starting a new venture, owning and operating a pharmacy. In order to increase the success, you have been asked to perform an enterprise risk assessment that includes reputational risk. Give three examples of how starting a new venture might have risk events that could lead to repercussions that would negatively impact the organizations reputation and three examples where it might be enhanced, creating opportunity.
2. Explain how improvement is measured with KPIs and give one example related to Human Capital and how this KPI might help you improve your organization.
3. In the UC example, the ERM Program gives weight to both data-driven activities and to culture-changing activities. Give two examples of each and then your own opinion regarding which activities you believe to be most effective in implementing an ERM program.
4. What do you think is the difference between *traditional risk management* and *enterprise risk management*?
5. From the UC example, identify what aspects of their program were "carrots" and which ones were "sticks." From your own experience describe which one you think works best in creating lasting change.

## NOTES

1. CRICO is the patient safety and medical liability company that serves the Harvard University medical community. It is a leader in evidence-based risk management.
2. Education in Legal Medicine.
3. UC Health, January 8, 2013.
4. http://webstore.ansi.org/phi.
5. http://workingsmarter.universityofcalifornia.edu/.
6. www.ucop.edu/finance-office/mission-goals/strategic-goals.html.

## ABOUT THE CONTRIBUTOR

**Grace Crickette** joined AAA Northern California, Nevada, and Utah (NCNU) in May 2013 as the Senior Vice President and Chief Risk and Compliance Officer. She was the former Chief Risk Officer at the University of California. In her current position, she is charged with implementing enterprise risk management (ERM) with her legal, compliance, risk management, and internal audit team. The Risk Services team provides internal audit and consultation, legal consultation, quality assurance and compliance, risk financing and captive solutions, crisis and consequence management, and loss prevention and loss control services. The Risk Services team's ERM vision is to support AAA's Membership Promise: "We will keep

you safe and secure—We will offer you the right product at the right time—We will provide you helpful and knowledgeable service—We will reward your loyalty—One Member, One AAA."

Prior to coming to AAA NCNU, Grace served as the University of California's Chief Risk Officer. Major initiatives for the Risk Services department included reducing the cost of risk, implementing system and local safety programs, improving claims management systems, developing risk financing strategies, and implementing enterprise risk management (ERM), and emergency management and business continuity planning throughout the university.

Grace joined the University of California in December 2004 after 13 years as a vice president and officer in audit, insurance, safety, and human resources capacities for the equipment and construction industry. She graduated with distinction from the University of Redlands with a bachelor's degree in business administration, and holds a variety of professional designations in the areas of claims, safety, audit, and human resources, including Associate in Risk Management and Senior Professional in Human Resources.

In 2008, Grace received the Risk Innovator Award for innovation and excellence in risk management in higher education. She received the Information Security Executive (ISE) of the Year West Award 2011 and National Award 2011 for Higher Education/Non Profit Sector for innovative problem solving related to a collaborative partnership with the University of California's chief information officer and other information technology (IT) professionals, insurance brokers, and underwriters for securing previously unavailable and much-needed cyber coverage and at the same time developing a program that will drive improvement and best practices into the future. She also received the ISE award of the decade for Higher Education/Non Profit Sector for her overall commitment to IT security. She was chosen in 2011 as one of *Business Insurance*'s Women to Watch, an annual feature spotlighting 25 women who are doing outstanding work in commercial insurance, reinsurance, risk management, employee benefits, and related fields, such as law and consulting. She was also selected by *Business Insurance* magazine for its 2011 Risk Management Honor Roll. Also in 2011, *Treasury & Risk* magazine named her one of the "100 Most Influential People in Finance." She has consulted with numerous public and private entities on the implementation of ERM, including Harvard University and SingHealth, Singapore's largest health care group.