Special Section: The Newest Frontier: Ethical Landscapes in Electronic Healthcare

Organizational Repertoires and Rites in Health Information Security

TED COOPER, JEFF COLLMANN, and HENRY NEIDERMEIER

The privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 emphasize taking steps for protecting protected health information from unauthorized access and modification.[1] Nonetheless, even organizations highly skilled in data security that comply with regulations and all good practices will suffer and must respond to breaches. This paper reports on a case study in responding to an important breach of the confidentiality and integrity of identifiable patient information of the Kaiser Internet Patient Portal known as ‘‘Kaiser Permanente Online’’ (KP Online). From the perspective of theories about highly reliable organizations, effective health information security programs must respond resiliently to as well as prospectively anticipate security breaches.[2]

In August 2000, legal counsel for Kaiser Permanente (KP) prepared a memo to members of the KP Online Situation Management Team summarizing conversations with counsel about an information security breach of KP Online. As analyzed elsewhere,[3] a technical glitch in a program designed to clear a backlog of replies to member queries in KP Online concatenated over 800 individual e-mail messages instead of separating them. After the first message, each message included the text of all preceding messages to multiple members, a flaw that caused a breach in the confidentiality and integrity of the members' personal health information. At least 19 of the e-mails reached their intended destination. Two members reported the breach, including one discussed in counsel's memorandum. In her memo, KP counsel describes the situation in terms of the characteristics of the breach as understood at the time, interaction with the member who reported the breach, initial plans for contacting affected members, and steps in understanding and mitigating causes of the KP Online breach. What does this memorandum teach about responding to organizational errors and failure? We hypothesize that this memorandum chartered and documents the mobilization of elements of KP's organizational repertoire to create sense in a situation that had become nonsensical. By ‘‘organizational repertoire’’ we mean embedded ethics (such as commitment to member well-being), resource individuals (such as KP legal counsel), and practiced procedures (such as creation of situational management teams) upon which an organization may draw at any

The authors thank staff at Kaiser Permanente for their review and comments on the paper. We also thank an anonymous reviewer from the *Cambridge Quarterly of Healthcare Ethics* for helpful comments on a earlier draft. The Georgetown University Institutional Review Board reviewed and approved the protocol for this study. An Interagency Personnel Agreement with the Telemedicine and Advanced Technology Research Center, U.S. Army Medical Research and Materiel Command, Ft. Detrick, MD, sponsored part of Dr. Collmann's work.

Cambridge Quarterly of Healthcare Ethics (2008), **17**, 441–452. Printed in the USA.

doi:10.1017/S0963180108080560

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

time to address problematic situations. The KP Online breach rendered problematic the ordinary, relatively unproblematic flow of business in the KP information technology program, particularly the development of web-enabled applications. In counsel's memo, we observe the beginning of a process that restores sense through a rite of transition that identifies and launches changes in the structure, management, and process of KP's entire IT program.

Background: The Disruption of Organizational Sense Making

Karl Weick explains that organizational sense making occurs as "[a]ctive agents construct sensible, sensable events" (p. 4).[4] Organizational sense making manifests multiple properties summarized as follows: "[P]eople concerned with identity in the context of others engage in ongoing events from which they extract cues and make plausible sense retrospectively, all the while enacting more or less order into those ongoing events" (p. 18).[5] The KP Online breach emerged from "compartmentalized sense making" during a period of major technical, managerial, and organizational transition in the Kaiser information technology program.[6] When faced with nonsense in the form of the disruptive breach, the KP Online critical incident response team stopped services, conducted an immediate investigation into the breach, launched a community relations campaign, and recommended multiple reforms in organizational procedures, management, and structure in an effort to restore organizational sensemaking.

Identity

The individual components of KP-IT maintained different work procedures that reflected deeper differences of identity.[7] The web development team (Web Development) focused on meeting the needs of their customers—specifically, pharmacists waiting for a new prescription application in KP Online and the KP members waiting for replies to their e-mails. As a development group with a project focus, Development felt driven by deadlines with relatively short-term time horizons. When problems emerged, project members strived to resolve them as quickly as possible using expedient, ad hoc methods. In contrast, the national operations team (Operations) focused on keeping their technology up and running according to standard operation procedures that had been learned and developed through years of experience in the mainframe environment. Operational uptime and established service level agreements, not project deadlines, drove their perception of urgency. Thus, Operations' approach to problem solving strictly followed standard procedures, with formal reviews and networks of accountability.

Ongoing Events

The KP Online accident unfolded as one of a series of cascading errors, accidents, and breaches in the context of major technical, management, and organizational transitions.[8] KP had recently completed integrating its regional IT infrastructures into a national enterprise information architecture. As illustrated by KP Online itself, Kaiser was beginning to experiment with early web-enabled technologies, a process conducted largely without input from traditional mainframe Operations,

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

its seat of historical IT experience and memory. In the middle of the KP Online development process, the KP enterprise architecture planning group (IT Planning) imposed a new web development platform on Web Development. As Web Development struggled with the new technology, it also experienced local organizational and managerial changes. With little experience in web technologies, KP-IT engaged outside contractors into the Web Development group. At the time of the breach, a new manager had assumed responsibility for the Web Development group but was still in transition. On the day of the breach, the contract project manager left town for the weekend and the current Web Development team leader was out with an illness. At multiple levels, the KP Online project existed betwixt and between—a situation ripe for the disruption of organizational sense making and failure.[9]

Cues and Retrospective Sense Making

The unanticipated and unintended consequences of the cascading accident functioned as cues that various KP-IT processes had gone awry. During the cascading accident itself, each cue emerged somewhat independently of the others and reflected the compartmentalized sense making characteristic of the various components of KP-IT at the time. These cues became starting points for the retrospective analysis of the KP Online incident management team as it began its investigation. This process culminated in two "root cause" analyses, one focusing on the late deployment of Rx Refill and the other focusing on the KP Online security breach. The root cause analysis of the failure to meet the Rx Refill deadline recommended, among other things, that all KP-IT problems be handled henceforth through the online Enterprise Support System, thereby documenting and attempting to replace the common practice of ad hoc problem-solving methods. The root cause analysis of the KP Online security breach made several recommendations with the aim of formalizing procedures in the Web Development unit according to established KP-IT principles.

These efforts to restore organizational sense making in the face of nonsense largely succeeded. Even before formulating a detailed picture of why the breach occurred, the KP Online incident response team developed and implemented a plan to call all affected members, explain what had happened, and suggest certain reparations. With few exceptions, the KP members accepted the call as evidence of Kaiser's good faith and basic competence. No lawsuits resulted from the case. The public press praised Kaiser's forthright response even as they reported the incident. The root cause analysis identified the immediate cause of the problem: flawed coding. KP disciplined no one because, like its members and the public press, it recognized the error as an expression of the programmers' commitment to their mission, not as evidence of incompetence or sloppy work. In conjunction with the recommendations of the root cause analysis, these actions rendered nonsense (the breach) sensible, reaffirmed core KP values and transitioned the KP-IT program to a new stage in its organizational maturity.[10]

Organizational Repertoire

We interpret the extended response to the KP Online breach as the mobilization of an organizational repertoire. By "organizational repertoire" we mean a range of more or less well-developed, more or less practiced, more or less widely disseminated approaches, procedures, or activities on which an organization may draw to help manage anomalous circumstances. In the KP Online case, we observe three elements of the KP organizational repertoire, namely embedded ethics (such as concern for member well-being), resource individuals (such as technical and cultural experts), and practiced procedures (such as critical incident response teams and root cause analyses). These are collective properties because they have been developed, practiced, and disseminated while solving organizational problems. The organizational repertoire constitutes a basic stock of resources for organizations to use in restoring sense to situations that have become nonsensical as a result of unexpected events.

Embedded Ethics

Embedded ethics are cultural values of the organization that can be observed by the way an organization conducts its activities. KP's response to the breach of KP Online included activities that demonstrate three specific embedded ethical values, namely concern for member well-being, aggressive internal organizational communication, and commitment to open business practices.

Concern for member well-being—KP employees are preoccupied with assuring the well-being of their members. Prompt, formal response to member e-mail malfunction: Recognizing the importance of prompt communication with members, KP-IT and KP Online business team had established a service level agreement requiring transmittal of messages within 24 hours. On July 24, 2000, it was noted that member questions sent via the KP Online member e-mail messaging function were not getting to the customer services center. Upon verification of the delay, KP-IT immediately assigned responsibility for resolving this malfunction. The KP-IT staff documented and monitored each step in the assessment and resolution of this malfunction using the online Enterprise Support System. Senior management focused attention on this effort because of its assigned high severity level.

Notification of all members affected by the breach of confidentiality: As documented in the memo from counsel, on the day that a member reported the breach of confidentiality, KP created a critical situation management team. This team decided to determine the identity of, notify, and develop a process to stay in touch with each individual member affected by the breach of confidentiality of personal health information.

Standardized process for communicating with affected members: Senior KP legal and KP Online business administrators developed standardized telephone and e-mail scripts to ensure that communication with members was accurate, complete, and responsive. The scripts acknowledged that KP Online breached the confidentiality of their personal health information (PHI) through a technical error. The scripts offered an apology for the error and expressed KP's wish to understand and address their concerns. An 800 toll-free number was established for members to respond to messages left on answering machines.

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

Senior staff made calls: The critical situation management team asked senior administrators, nurses, and physicians to contact members affected by the breach depending on the sensitivity of the PHI involved.

Aggressive internal communications—KP employees aggressively raise the alarm upon discovering a problem. Member Services Call Center Alerted KP-IT of PHI breach response: Upon receiving the member's report, the member services call center immediately recognized the KP Online breach as a significant information technology issue and promptly notified KP-IT by telephone. This communication occurred even though the call center had never before received a call of this nature. They usually received requests to schedule or cancel appointments or to take messages for providers.

KP-IT staff sustained the chain of communication: Immediately on being notified of the breach of member PHI confidentiality, KP-IT notified the KP Online business team by telephone. In its turn, the KP Online business team immediately contacted the CEOs of KP and the Permanente Federation. As described at the beginning of this article, senior counsel chartered and documented the work of the KP Online Situation Management Team through a memo to its members with copies to the CEOs of KP and the Permanente Federation. This pattern of open communication persisted throughout the crisis.

KP-IT uses an automated "trouble ticket" information system: KP-IT used an online Enterprise Support System for internal communication, management, and tracking of efforts to address technical aspects of all its computer and network operations problems. As described above, this practice supports member well-being through prompt response to member-related issues. It also demonstrates a commitment to open communication across the enterprise because this software was available to all KP-IT staff on any workstation attached to the KP network. The recommendations flowing from review of this incident included requiring the Web Development division of KP-IT to begin using the online system to track all "trouble tickets."

Open Business Practices—In Order to Maintain Trust with Its Members and the Public, KP communicates openly about its business practices, including its errors. KP took three steps to communicate the KP Online breach to outside audiences.

Prompt notification of affected members: The critical situation team immediately recognized the potential for the KP Online breach to harm members and negatively affect the reputation of KP. To mitigate this potential their initial concern was the notification of the members of the breach of their PHI. As explained in the memo from counsel, they organized a comprehensive plan to call, support, and respond to all members implicated in the breach of PHI.

Prompt reporting of such situations to regulatory agencies: The critical situation team also reported the breach to all relevant regulatory agencies. Although the draft HIPAA security rules were under public review in 2000, KP made this disclosure to regulatory agencies on its own volition, not in response to a regulatory mandate.

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

Prompt disclosure of the incidents to the public media: The critical situation team also held a press conference to publicly acknowledge the KP Online breach. Reports of the breach appeared in major newspapers across the United States, including the front page of the *Washington Post*.[11]

Resource Individuals

An organization's repertoire includes individuals with technical and cultural expertise from whom to recruit assistance in managing nonsensical situations.

KP mobilized relevant technical experts as dictated by the problem. The technical issues involved in both the malfunction of the KP Online e-mail failure and restoration of the e-mail messages from the dead letter file posed complex infrastructure, application, and programming questions and, thus, required technical expertise from several different sections of KP-IT. KP-IT division managers assigned individuals with the most appropriate technical skills and experience to investigate and resolve these problems. In the case of the e-mail failure, these teams included technical staff who routinely worked together. Clearing the dead letter file, however, required assigning programmers from separate divisions who had never worked as a team before. They had to pool their efforts because no KP-IT staff member or division had the complete knowledge necessary to fix the problem.

KP mobilized cultural and organizational expertise when managing technical failures. The KP Online security breach occurred as part of a cascading system accident that included multiple technical and organizational failures.[12] Kaiser acknowledged the multidimensional nature of these failures by assigning staff with cultural as well as technical expertise to their investigation. The KP Online critical situation response team consisted of over 15 members including the KP online business manager, several attorneys, a physician, healthcare operations administrators, and information technology professionals. Some members of this team displayed technical and programmatic knowledge of KP Online. Others demonstrated cultural expertise through their understanding of Kaiser's values with respect to its members, clinical practice, crisis management, and public relations. KP-IT assigned a senior information technology architect to conduct a "post-implementation review" of the delayed implementation of the new prescription refill functionality for KP Online, a delay that contributed to the e-mail malfunction and security breach. The postimplementation review team identified the "root technical cause" of the delays but also highlighted several even more significant problems of business process and organizational structure among the KP-IT divisions that put the entire KP Online program at risk if not corrected. The team documented lessons learned and developed an action plan for resolving the technical and cultural problems.

Experienced legal counsel guided response. As documented in the memo from counsel described above, KP assigned legal counsel with prior experience in managing unexpected events (crises) to guide the response to this incident. Although well versed in the law, counsel functioned broadly as a senior expert in Kaiser

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

embedded ethics and values, resource individuals, and practiced procedures—all of which are expressed in the chartering memo.

Practiced Procedures

In its years of experience managing large data centers based on mainframe computer technology, Kaiser learned many lessons and practiced many procedures for addressing critical incidents. Our informants about the KP Online breach repeatedly observed that the Web Development team applied few of these lessons while trying to incorporate innovative web technology into Kaiser's work. Yet, we observe that, when faced with nonsense emanating from the Web Development group's work, KP-IT invoked well-practiced procedures, in particular its mobilization of critical incident management teams, and began applying them to this anomalous area. Before the end of the work day on which the KP Online security breach became known, Kaiser had created a critical incident response management team. As we have already observed, this team expressed embedded Kaiser ethics, recruited technical and cultural experts as members, and implemented various specific procedures that Kaiser routinely used to manage comparable incidents. To conduct the root cause analysis of technical failures underlying the breach and delayed Rx Refill implementation, Kaiser invoked a robust postimplementation review process that bears great resemblance to the critical situation response team. The Kaiser organizational repertoire certainly included practiced incident management procedures even if the KP Web Development team ignored disciplined development procedures.

Organizational Rite of Transition

Anthropologists commonly identify certain religious ceremonies as rites of passage or transition. Rites of transition exhibit a typical, well-known form that includes moments of segregation, liminality, and reaggregation.[13] As individuals move through the steps of rites of transition, they move from one life stage to another, becoming different persons as a result of the process. We hypothesize that as Kaiser Permanente mobilized its organizational repertoire to address the various dimensions of the KP Online failure, its activities took the form of an organizational rite of transition focused on restoring the conditions for organizational sense making with respect to relationships among their workgroups and their members. Although occurring in the context of a bureaucratic rather than a sacred frame of reference, KP's activities took participants out of their everyday work routine (segregation), reflected upon and reaffirmed the ethical foundations of Kaiser's relationships with its patients as well as its work process (liminality), and created recommendations designed to change the managerial process and organizational structure of KP-IT (reaggregation). In the course of this process, authoritative KP administrators exonerated various individuals of blame for their mistakes and blessed others for their efforts to restore order. These cases suggest that mobilizing the organizational repertoire to address failure and nonsensical situations through bureaucratic rites of transition constitutes an important and adaptive feature of Kaiser corporate culture.

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

Segregation

Declaration of two KP Online-related crisis management teams established the situation and their work as outside the ordinary flow of bureaucratic life at Kaiser, particularly for the team managing the security breach. As soon as news of the KP Online breach began to disseminate throughout the organization, KP assembled a crisis management team of expert and responsible individuals, who suspended their normal work and refocused all their attention on the situation. These individuals did not routinely work together. A few but not most of the crisis team members actually worked on the KP Online project. They did not represent people to whom KP assigned routine crisis management responsibilities. Some made a forced return from leave, expressing a sense of urgency uncharacteristic of ordinary project life. All worked over the weekend to develop a response. The nonsensicality of the breach created an organizational hiatus out of ordinary bureaucratic time and space that KP peopled with the crisis management team who thus left their own ordinary temporal and spatial niches. In a similar if less dramatic fashion, members of the Rx refill postimplementation review team also interrupted their everyday activities to reflect on the reasons for the application's late launch.

Liminality

The security breach and late delivery of the Rx Refill application clashed dramatically with KP's expected mode of operations. The crisis management teams examined and proposed action to reduce these inconsistencies between the real and the ideal during their deliberations. These deliberations about the ethical foundations of Kaiser life among resource individuals mobilized in the practiced procedure of crisis management occurred "betwixt and between" undesirable nonsensical failures and restored organization sense making. Their deliberations addressed the structural conditions along the four dimensions of compartmentalized sense making then prevailing in KP-IT, including the following.

Identity: The postimplementation review team directly addressed the problem of the differing work procedures and identities among the various components of KP-IT in its "Summary of Lessons Learned." Four lessons bear special notice. Lesson 1 reads: "Effective QA and stress testing prior to production requires that development, QA and production environments be as similar as possible and gaps well-understood." Lesson 3 reads: "Effective response to unanticipated problems requires close teamwork between KP-IT internal organizations." Lesson 7 reads: "Disagreements within KP-IT over standards must be resolved early (i.e., Weblogic versus Websphere)." Lessons 8 reads: "New technology requires special attention across the organization." Taken individually and together, these lessons articulate and condemn the effects of Web Development, Operations, the E-mail group, and the IT Planning group each maintaining its own separate identity, work procedures, and priorities. Thanks to these clashes, KP-IT failed to meet its internal customers' needs for timely delivery of a new application and harmed patient members through a breach of their privacy, both violations of core-embedded KP ethical values. The essential recommendation follows that the various components of KP-IT must surrender their individuality and work as a team.

Ongoing events: These and other lessons also addressed the major technical, management, and organizational transitions that were occurring in KP-IT at the

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

time of the failures. Lessons 6 reads: “KP-IT must become self-sufficient in supporting complex, multi-vendor applications.” This lesson refers to the fact that KP-IT at the time had an overreliance on third-party consultants in web application development. As development platforms changed, the third-party consultants also changed, yielding general uncertainty and incidental but important errors such as untimely expiration of contracts and the failure of support at critical moments. The night of the KP Online security breach, no manager with requisite knowledge or experience was available to help either from KP-IT or the third-party vendor. The essential recommendation of this lesson follows: Install mature system development processes with appropriate testing.

Cues and retrospective sense making: The KP Online security breach and late delivery functioned as cues to the disruption of sense making in the KP Online development process and, thus, became starting points for the retrospective analyses of the crisis management teams. They articulated many lessons learned. Some were new, such as the lessons about web development explained above. Others reaffirmed embedded Kaiser values. In a study of Kaiser’s response to the security brief, a student in a Masters in Public Health program outlined these key lessons learned. In managing a breach, an organization should

- Be honest with its customers when a mistake is made.
- Keep top management informed so that they fully support the strategy.
- Communicate within the organization.
- Consider a proactive approach with the media.
- Conduct a root-cause analysis.
- Fully support the people who work the crisis.

We see all these “lessons learned” as elements in the organizational repertoire of Kaiser Permanente mobilized during its response to the KP Online security breach and late delivery. By the time the teams had finished their deliberation, they recognized the fundamentally organizational basis for KP Online’s difficulties. Although they acknowledged that certain individuals made errors, they refused to blame them. Rather, they recognized that a failure of teamwork and process among the KP-IT units during a time of technical, managerial, and organizational transition as the true origin of the problems.

Reaggregation

Reflecting on events later, two persons intimately involved with the response to the breach made separate but comparable assessments. The KP Online program manager stated, “We had no mitigation plan because this was the adolescence of web development. People thought you could abandon everything you knew in conventional IT because this was the web” (personal communication). The person who assumed responsibility for Web Development just after the security breach described the event as an organizational epiphany and turning point. She noted that, thanks to the security breach, they became aware of KP Online’s value and risk. Quoting from the postimplementation review team’s report, she observed how they had to end web development group’s isolation from the rest of KP-IT by imposing standard corporate IT discipline on its work process, hiring

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

more people, and working on building trust between the Web Development and Operations staff. The problem, she argued, was KP-IT's overall maturity with respect to web technology and patient information. She said, ''The IT organization was not mature with respect to web technology. We did not realize the brevity of our support. If we had, we'd have had a disaster recovery plan. To create a disaster recovery plan document, you had to pull away from working on items in the queue. That's a perennial challenge for IT: Development competes with production. If you don't have processes in place, you will fail'' (personal communication). Thankfully, they both noted, KP-IT had instituted an incident management process, on-call procedures, and other contingency plans. The KP Online program manager stated, ''Today this wouldn't happen because we have an on-call system. We are always evolving. We keep reviewing. We now have a whole new system with split calls and subspecialists in incident response'' (personal communication). Both persons use the language of growth and development. The Web Development team was ''adolescent,'' ''immature,'' and indifferent to the lessons of its elders. The breach taught them the error of their immature ways. Having realized their state of immaturity, KP-IT passed through an organizational life crisis to the next stage in its maturity.

Benediction. Reflecting on her experience during the KP Online crisis, a senior KP-IT engineer told us

> I enjoyed the conversation (with the authors) yesterday although it brought back a rather painful time. I do have to say that I was very proud of the way Kaiser responded to this event; not many organizations would have been as honest and ethical. Best of all, I remember all of us involved being called to (the Kaiser CEO's) office and instead of being bawled out, we were thanked. He thanked us for all the work in cleaning up the problem and, most of all, he thanked us for pushing the envelope in putting up the KP Online system. He said he understood we were driving towards the future and mistakes would be made; it was important to own them, fix them and not to let them stop us moving forward. It was one of my proudest moments as a Kaiser employee. (personal communication)

Like a priest at the end of mass, the Kaiser CEO offered a benediction to his faithful staff upon closing the transition from disrupted to restored organizational sense making in the KP Online program. Through his words, he reaffirmed the core organizational value of using technological innovation for the benefit of Kaiser's members. As a source and embodiment of Kaiser's cultural universe, he validated his staff's identities as vital and effective members of that universe. As long as they kept the faith, practiced sound doctrine, and continued the struggle for progress, he exonerated them from blame for errors. With these words, he sanctified their efforts and enabled them to return to work revitalized as sensible members of the community.

Conclusion

From the perspective of HIPAA, the need for incident security policies and procedures constitutes one required standard among many.[14] At the time of the

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

KP Online incident, KP had no specific IT security response plan but, instead, drew from its broader organizational repertoire that included embedded ethics, resource individuals, and practiced procedures readily available and adaptable to the situation. Within hours, KP mobilized an experienced critical incident management team, formulated a plan for contacting affected members, approached the media, and corrected the technical failure. KP mobilized a model security incident response from which most healthcare organizations could learn when designing or evaluating their information security compliance plan.

From the perspective of high reliability theory, however, the lessons of KP's response to the KP Online breach go beyond regulatory compliance. Organizations with rich incident response repertoires demonstrate much greater resiliency than those with impoverished response repertoires because they demonstrate ''a state of collective mindfulness that creates a rich awareness of discriminatory detail and facilitates the discovery and correction of errors capable of escalation into catastrophe'' (p. 81).[15] When failure strikes, such organizations deploy experts close to the problem to restore effective performance. These experts aggressively seize, exhaustively investigate, and seek explanations of failures in daily operations. In mobilizing its organizational repertoire to address the various dimensions of the KP Online failure, KP demonstrated characteristics of a mindful, highly reliable organization even though its IT program had suffered a major failure.[16] KP survived the KP Online breach with its membership and reputation intact because of these basic characteristics.

KP lent added significance to high reliability theory by giving its assessment and resolution activities a processional form that changed their investigations from mere fact-finding missions into exercises in organizational transformation. In the years following the events reported here, KP launched a major effort to enhance the reliability of its entire IT program. Having come through this rite of passage relatively unscathed, it treated the incident as a near miss, a bad accident that could have been much worse. Instead of breathing a collective sigh of relief and closing the books on the breach, it displayed collective mindfulness and recognized areas of its total performance that needed reform. Of all the lessons learned from the KP Online breach, perhaps this emerges as the most important—treat all accidents as near misses alerting an organization of the need for change. As healthcare organizations throughout the world deploy electronic health records, they will almost certainly experience breaches that engender unexpected and nonsensical situations. To successfully address such incidents, healthcare organizations would do well to develop rich organizational repertoires through embedding their culture, people, processes, and technology with the characteristics of high reliability and an ethos of continuous development.

Notes

1. Health Insurance Reform: Security Standards; Final Rule. 68 Fed. Reg. 8333-8381 (Feb 20, 2003); Standards for Privacy of Individually Identifiable Health Information. 65 Fed. Reg. 82461–82829 (Dec 28, 2000).
2. Weick K, Sutcliffe K. *Managing the Unexpected: Assuring High Performance in an Age of Complexity.* San Francisco, CA: Jossey Bass; 2001; Weick K, Surcliffe K, Obstfeld D. Organizing for high reliability: Processes of collective mindfulness. *Research in Organizational Behavior* 1999;21:81–123.
3. Collmann J, Cooper T. Breaching the security of the Kaiser Permanente Internet Patient Portal: The organizational foundations of information security. *Journal of the American Medical Informatics Association* 2007;14:239–43.

https://doi.org/10.1017/S0963180108080560 Published online by Cambridge University Press

4. Weick K. *Sensemaking in Organizations*. Thousand Oakes, CA: Sage Publications; 1995.
5. See note 2, Weick 1995.
6. See note 3, Collmann, Cooper 2007.
7. Snook S. *Friendly Fire: The Accidental Shootdown of US Black Hawks over Northern Iraq*. Princeton, NJ: Princeton University Press; 2000.
8. Perrow C. *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press; 1999.
9. Turner V. *Drama, Fields and Metaphors: Symbolic Action in Human Society.* Ithaca, NY: Cornell University Press; 1974.
10. Paulk M, Weber C, Curtis B, Chrissis M. *The Capability Maturity Model: Guidelines for Improving the Software Process*. Boston, MA: Addison Wesley Professional; 1995.
11. Brubaker B. "Sensitive" Kaiser e-mails go astray. *Washington Post* 9 Aug 2000.
12. See note 3, Collmann, Cooper 2007.
13. Turner V. *Schism and Continuity in an African Society*. Manchester, UK: Manchester University Press; 1957; Kapferer B. *A Celebration of Demons: Exorcism and the Aesthetics of Healing in Sri Lanka*. Washington, DC: Smithsonian; 1991.
14. See note 1, Health Insurance Reform 2003.
15. See note 2, Weick et al. 1999.
16. See note 2, Weick, Sutcliffe 2001.