Case Report  ■

Breaching the Security of the Kaiser Permanente Internet Patient Portal: the Organizational Foundations of Information Security

JEFF COLLMANN, PHD, AND TED COOPER, MD

Abstract This case study describes and analyzes a breach of the confidentiality and integrity of personally identified health information (e.g. appointment details, answers to patients’ questions, medical advice) for over 800 Kaiser Permanente (KP) members through KP Online, a web-enabled health care portal. The authors obtained and analyzed multiple types of qualitative data about this incident including interviews with KP staff, incident reports, root cause analyses, and media reports. Reasons at multiple levels account for the breach, including the architecture of the information system, the motivations of individual staff members, and differences among the subcultures of individual groups within as well as technical and social relations across the Kaiser IT program. None of these reasons could be classified, strictly speaking, as “security violations.” This case study, thus, suggests that, to protect sensitive patient information, health care organizations should build safe organizational contexts for complex health information systems in addition to complying with good information security practice and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996.


Case Description

Serving over eight million members in nine states and the District of Columbia, Kaiser Permanente (KP) functions as an integrated health delivery system. In 1995 the KP Northern California region funded an innovation project to create an Internet Patient Portal known as “Kaiser Permanente Online” (KP Online). Using KP Online, patients may request appointments and prescription refills, obtain information on KP health care services, seek and receive medical advice from nurses and pharmacists, and participate in professionally moderated forums. In 1997 KP funded a program to extend KP Online nationally to all patients. The pilot project staff transferred to the national level to do this.

During the time KP Online emerged, KP reorganized IT management from 13 regionally-based IT services to a single nationally-based organization (KP-IT) with its own senior KP vice president. KP-IT incorporated existing and new departments. Four units were involved with KP Online: National Operations (Operations), E-mail and Groupware Services (E-mail), Web Portal Services (Development), and Enterprise Planning and Architecture (IT Planning). These four units of KP-IT differed in their missions, domains of technical expertise, and managerial styles. In addition to this major reorganization, KP introduced new technology—such as workstations, networks, the Internet, e-mail, and groupware applications—upon which health care workers and health plan members came to depend. This mix of technical and operational reorganization created discontinuities that, among other errors, produced the KP Online security breach.

In August 2000, an Operations technician applied patches to servers in support of a new KP Online pharmacy refill application. Subsequently, the outgoing e-mail function of KP Online failed and created a deadletter file of outbound messages with replies to patient inquiries that contained individually identifiable patient information. In trying to clear the e-mail deadletter file, two programmers wrote a flawed computer script that 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 nineteen of the e-mails reached their intended destination. Two members who received concatenated messages reported the incident to Kaiser Permanente. Kaiser considered this breach a significant incident given the number of errant messages sent and the amount of improperly disclosed personal health information. An investigation, apologies, and organizational reform followed (see Figure 1).

Methods

This case study follows the long tradition of ethnographic research that focuses on extended “trouble cases.” Trouble cases have the virtue of exposing the taken-for-granted principles of everyday life normally obscured by
the apparently unproblematic patterns that drive routine living. This study is also informed by the literature regarding organizational error in complex technological systems. While acknowledging the structural difficulties of managing complex systems, “High Reliability” or “High Resiliency” theorists (HRT) argue that strong leadership, continuous training and practice, redundant safety mechanisms, and organizational mindfulness create cultures of safety that prevent catastrophic accidents and allow organizations to learn from their mistakes. Normal Accident Theorists (NAT) argue that complex, tightly coupled systems inevitably produce system accidents that are difficult if not impossible for human operators to manage. Complex systems include many diverse components interconnected in multiple ways. Tightly coupled systems exhibit few gaps enabling rapid system operation and process flow, and, in the event of error, allowing local human and technical failures to escalate into larger-scale accidents with implications for the system as a whole. Thus, complex, tightly coupled systems often preclude even well-trained operators from effectively tracking and preventing system accidents with catastrophic consequences. The Kaiser IT program illustrates elements of both perspectives: Kaiser pioneered the application of complex, interconnected information technology to health care within a nationally recognized program of good information security practice. This study also employs categories of analysis developed by Scott Snook, who described one trouble case, the shootdown of U.S. Army Blackhawk helicopters by U.S. Air Force jet fighters during Operation Provide Comfort. Snook argues that understanding complex accidents requires analyzing conditions at the individual, group, and organizational levels of social analysis. Thus, he analyzes the actions of the fighter pilots who took the shot, the subcultures of the various groups involved in the incident, and the organization of Operation Provide Comfort itself. For both the Blackhawk shootdown and the KP Online breach, failure was precipitated by a mixture of competent and flawed performance, as well as by improvised and standard procedures at all levels. To provide a
full explanation of the shootdown, however, Snook developed a cross-level concept, “practical action,” that accounts for events at all levels as a function of dynamic organizational processes unfolding over time. According to Snook, “practical action” operates as a ubiquitous feature of organizational life and refers to “behavior that is locally efficient, acquired in practice and legitimized through unremarkable repetition.” When “practical action” works on formally planned operations such as Operation Provide Comfort, it creates “practical drift,” or the “slow steady uncoupling of practice from written procedure.” The shutdown occurred when organizational processes in Operation Provide Comfort that had been drifting apart suddenly reintegrated. In the KP Online case, we observed practical action inhibiting full implementation of planned organizational reforms that, when combined with the highly integrated KP IT infrastructure, created the possibility for the accident. We note, particularly, discontinuities between the “development” and the “production” sides of Kaiser’s IT program. Because the information technology architecture of KP Online played such a significant role in the development of the accident, we have drawn upon Perrow’s work to analyze the technical level.

The Institutional Review Board of Georgetown University reviewed and approved this study. KP granted us permission to study the KP Online breach using multiple sources and types of data about the incident (data triangulation). They provided us with key documents, such as the post-implementation review of the RxRefill installation (new KP Online functionality), the minutes of KP Online crisis team meetings, a summary of the root cause analysis of the KP Online breach, and the complete text of the KP Incident Management System that describes each technical step taken to address the failure. KP also allowed us to interview key personnel who were involved in the breach, including programmers and managers from all the units of the KP national information technology organization. Additionally, we reviewed newspaper reports of the incident early on in our research. Finally, KP personnel have reviewed this analysis and adopted it for use in their staff training program (member checking). The investigators remain entirely responsible for the opinions and analysis expressed in this case study.

Example
A full understanding of the KP Online breach requires technical, individual, group, organizational, and cross-level analysis.
Technical Level: The Architecture and Management of the Kaiser IT Infrastructure

Two individuals made specific mistakes that led to the immediate breach of message security. However, they did so within a complex, tightly coupled, Internet-based information system (see Figure 2). Thus, when they placed the flawed program into the production environment, messages flowed through the KP Online system without interruption.

Responsibility was fragmented for the various components of KP Online. As Figure 2 illustrates, multiple applications and systems were used to send and receive e-mails through KP Online. All these components functioned as parts of the overall Kaiser Permanente information technology infrastructure for which a national organization, KP-IT, bore official responsibility. Nonetheless, distinct units within KP-IT managed each technical area. The Development group designed, instrumented, tested, and managed the KP Online application. The E-mail group managed KP e-mail applications as well as a central mail hub. The Operations group managed the hardware, operating systems, and network that supported both e-mail and Web services. Although the groups relied on each other’s work as they implemented pieces of the entire KP Online transaction, they did not help each other develop, test, or manage their respective technologies. In particular, the Development and E-mail groups developed their programs with little assistance or guidance from their parent organization, KP-IT, until IT Planning began imposing corporate Web server standards on KP Online.

New technology compounded the problems caused by fragmented responsibility. By building KP Online with Web-enabled technology, Kaiser was experimenting with novel tools, applications, and processes. Moreover, at the time of the KP Online accident, Development was also transitioning from a familiar to a new and unfamiliar Web development platform at the insistence of IT Planning. Although a Development programmer had evaluated the pharmacy module in the Development test environment, the effect of these changes could not be predicted because the test and production environments were not equivalent, a situation discovered only after the accident.

Individual Level: Circumstances of the Technical Staff Who Committed the Programming Error

At the individual level, the two programmers, one from E-mail and another from Development, faced a challenging set of circumstances. One understood the programming language and the other understood the application environment necessary to fix the problem. Never having worked together before, they nonetheless cooperated to address the problem in an ad hoc environment. Unable to write code in the e-mail production system, they prepared and launched the flawed program in Development’s testing environment that they had temporarily linked to the production e-mail system, an arrangement they knew was generally prohibited by KP-IT. On the other hand, they faced intense pressure to quickly clear the deadletter file. Even though they knew they should rigorously test new code, they executed only a “desk check” that missed the bug in the program. They believed that the organization placed a higher priority on clearing the deadletter file than on following standard procedures, a belief confirmed in interviews with E-mail and KP Online administrators. Because of these conditions, the two programmers combined to make an “error” that escalated into an “accident.”

Group Level: Differing Subcultures of the KP-IT Component Groups

Operations, E-mail, and Development had historically evolved independently with distinct missions, operational priorities, customer focuses, and work styles. They routinely worked with distinct technologies upon which they built their own group work processes, identities, and ideologies. The contrasts between Operations and Development could not have been much greater at the time of this accident. Operations perceived their role as keeping KP’s computer systems and networks up and operating properly. They had developed and implemented disciplined standard procedures for development, testing, and troubleshooting. They adopted a cautious attitude to innovation and viewed the newly emerging World Wide Web as a potential threat to their mission. Development perceived itself as using the latest technology to provide new services to Kaiser Health Plan members, services that the mainframe environment did not yet support. They had adopted a fluid work process with few standard procedures. Strong on innovation but weak on established discipline, meeting deadlines for new applications dominated their sense of priorities. They functioned like a “skunkworks” with situation-driven procedures and in relative isolation from other components of KP-IT, particularly Operations. Operations functioned using well-defined policies and procedures while Development functioned in an ad hoc manner. E-mail shared some of the characteristics displayed by Operations and Development. The KP Online business team had to negotiate the implications of these different approaches. On a daily basis, they interacted with the Development group. When the accident occurred, they discovered their dependence on as well as the differences among all three groups.

Organizational Level: Compartmentalized Sensemaking in KP-IT

When the Operations programmer installed patches on the KP Online e-mail server in preparation for launching the Rx-Refill application, it reverberated throughout the KP e-mail system causing a series of errors including but not limited to the breach of information security, an event that Perrow labels a cascading system accident. Although the complex, tightly coupled characteristics of the Kaiser IT infrastructure ensured rapid propagation of the errors, the real roots of the system accident originated in organizational rather than technical complexity. We interpret KP-IT’s organizational complexity as the result of compartmentalized sensemaking. Karl Weick explains that organizational sensemaking occurs as “Active agents construct sensible, sensible events.” While sensemaking constitutes a core activity for all persons working in organizations, each KP-IT group developed highly localized definitions of the situation that created the possibility for failure when integrated in a common infrastructure. The focused, context-specific problem-solving of each KP-IT group produced unanticipated, disruptive consequences for other KP-IT departments to address. Thus, as Kaiser began to integrate the disparate components of its emerging IT program, boundaries hard-
Cross Levels: The Consequences of Technical Conjunction and Organizational Disjunction

The KP Online accident occurred at a point of technical conjunction but organizational disjunction during KP-IT’s process of overall organizational integration. The anthropologist Radcliffe-Brown emphasizes the generative possibilities of points of conjunction and disjunction depending upon the relative power distribution between interacting parties.20 As (partially) subordinate and technically dependent components of KP-IT, E-mail and Development should have deferred to its policies, procedures, and established practices as implemented by Operations. Their program authority and technological expertise, nonetheless, established E-mail and Development as peers if not superiors to Operations with respect to Web-enabled applications. Avoidance marks such structurally ambiguous relationships. Thus, we observe that, as these work units tactically maneuvered to discharge their respective missions (compartmentalized sensemaking), they basically avoided each other and, thus, produced a series of errors, including but not limited to the security breach of patient messages in KP Online (Figures 1 & 2).

Discussion: Lessons Learned from KP Online Breach

This case study offers cautionary lessons for health care administrators as well as areas for further research.

1. Complex, tightly-coupled computerized health information system architectures potentially aggravate security breaches or other mistakes with their capacity to transform errors into cascading system accidents.

2. Security training is necessary but not sufficient to prevent information security breaches because individual errors, group failures, and system accidents may contribute to information security breaches without violating the HIPAA security rules or standard information security policies, procedures, or practices.

3. Breaches of health care information may signify broader organizational discontinuities and failures to which health care administrators should attend, particularly during periods of reform or transition in an IT program.

4. Although ISO 17799,21 HIPAA,22 and other regulatory regimes are forcing health care organizations throughout the world to pay increasing attention to good information security practices, protecting health information also requires fostering general good information management practices such as change control, routine inter- and intradepartmental communication, and comprehensive failure analysis that transcend the domain typically labeled “information security.”

References


3. Collmann J. I’m proper number one fighter, me!: Women’s gender roles & bureaucracy among Aboriginal fringedwellers. Gender & Society 1988;2(1).


