*Research Paper* ■

# Giving Patients Access to Their Medical Records via the Internet:

## The PCASSO Experience

DANIEL MASYS, MD, DIXIE BAKER, PHD, AMY BUTROS, MLS, KEVIN E. COWLES

**Abstract** **Objective:** The Patient-Centered Access to Secure Systems Online (PCASSO) project is designed to apply state-of-the-art-security to the communication of clinical information over the Internet.

**Design:** The authors report the legal and regulatory issues associated with deploying the system, and results of its use by providers and patients. Human subject protection concerns raised by the Institutional Review Board focused on three areas—unauthorized access to information by persons other than the patient; the effect of startling or poorly understood information; and the effect of patient access to records on the record-keeping behavior of providers.

**Measurements:** Objective and subjective measures of security and usability were obtained.

**Results:** During its initial deployment phase, the project enrolled 216 physicians and 41 patients; of these, 68 physicians and 26 patients used the system one or more times. The system performed as designed, with no unauthorized information access or intrusions detected. Providers rated the usability of the system low because of the complexity of the secure login and other security features and restrictions limiting their access to those patients with whom they had a professional relationship. In contrast, patients rated the usability and functionality of the system favorably.

**Conclusion:** High-assurance systems that serve both patients and providers will need to address differing expectations regarding security and ease of use.

■ **J Am Med Inform Assoc.** 2002;9:181–191.

The Patient-Centered Access to Secure Systems Online (PCASSO) project is designed to apply state-of-the-art security to the communication of clinical information over the Internet. When the project began in 1996, several prototype Web-based clinical information systems existed,[1–5] but these were explicitly designed to serve only health professionals, and most used security "firewalls" to filter queries originating from outside an organization's private network.

PCASSO was conceived with the premise that the full potential of a ubiquitous national information infrastructure (NII) lies in its catalysis of new and expanded opportunities for communication, not simply in the acceleration of existing lines of communication. A key theme of the NII is individual empowerment, a focus on the "customer" as a participant and partner in the flow of information. In a medical environment, this customer is the patient, who is empowered by PCASSO technology to access his or her own health information.

The PCASSO security model explicitly recognizes the rights and responsibilities of providers and their patients, and implements those rights and responsi-

Affiliation of the authors: University of California, San Diego, La Jolla, California.

Correspondence and reprints: Daniel Masys, MD, Director, Biomedical Informatics, UCSD School of Medicine, 9500 Gilman Drive, Mailcode 0602, La Jolla, CA 92093-0602; e-mail: <dmasys@ucsd.edu>.

Received for publication: 8/14/01; accepted for publication: 11/19/01.

bilities through a role-based access-control scheme that enforces confidentiality, integrity, and accountability rules compatible with public data networks such as the Internet. The technical details of the system design, including the overall architecture,[6] the security model and concept of operations,[7] the approach to overcoming client-side vulnerabilities,[8–10] and methods for attaining high assurance of correct operations[11] have been described elsewhere. Here we report the legal and regulatory issues associated with deploying the system, and the results of its use by providers and patients associated with the University of California, San Diego (UCSD) Healthcare, during calendar year 1999.

## Legal and Regulatory Context

The legal and regulatory context for the PCASSO project included existing and emerging federal and state laws and regulations regarding health information security and patient privacy, as well as Institutional Review Board (IRB) regulations regarding the use of human subjects in research activities.

The PCASSO vision, as described in the initial project plan, was to capitalize on state-of-the-art security technologies and the ubiquity of the Internet to enable patients and their providers to view patients' medical records from virtually anywhere. The legislative authority and mandate for doing this in the State of California is contained in the California Health and Safety Code, which states that:

> The Legislature finds and declares that every person having ultimate responsibility for decisions respecting his or her own health care also possesses a concomitant right of access to complete information respecting his or her condition and care provided.[11]

The Code defines both a general right of access and several special circumstances for denying or restricting patients' access to their health records, including health records of minors, alcohol and drug abuse treatment records, mental health records, and records describing communicable disease carriers. The California statutes entitling patients to full access to their records are similar to statutes found in approximately 20 other states, but the variability among states' laws also extends to the opposite extreme, where seven states specifically deny patients the right to see medical records, and three additional states allow patients to see only mental health records.[12]

Since the start of the PCASSO project, health care has experienced significant change in the areas of information security and patient privacy, primarily prompted by the Health Insurance Portability and Accountability Act (HIPAA) of 1996,[13] which called for the development and implementation of a number of standards, including security and privacy. The Privacy Standard,[14] which went into effect in April 2001, set forth the rights of individual patients with respect to the access to and use of their protected health information, thus establishing a uniform, minimum set of patient rights nationwide. However, because states still may enact laws that extend the rights to patients beyond what is specified in the Privacy Standards, variability remains.

The draft Security Standard issued pursuant to HIPAA[15] specified requirements covering administrative practices, physical safeguards, and technical services and mechanisms. The draft standard was issued in August 1998; the Department of Health and Human Services has announced final issuance by the end of 2001.

In November 1998, the U.S. Centers for Medicare and Medicaid Services (CMS, formerly Health Care Financing Administration) released technical guidelines for the acceptable use of the Internet to communicate person-identifiable health information.[16] The guidelines specify that all CMS information protected by the Privacy Act and other sensitive CMS information may be transmitted over the Internet so long as an acceptable method of encryption is used to protect confidentiality and integrity, and authentication or identification procedures are employed to ensure that both the sender and the recipient of the data are known to each other and are authorized to receive and decrypt such information.

## Methods

### The PCASSO Model and User Experience

The PCASSO model was built using high-assurance methods that have been described previously.[10] The architecture includes an application server to which the UCSD clinical information systems pass data in HL7 messages. These messages are parsed and stored in PCASSO's clinical data repository (CDR), labeled at one of five sensitivity levels—low, standard, public-deniable, guardian-deniable, and patient-deniable. "Low" data are not patient-identifiable, such as data that have been de-identified in accordance with the HIPAA Privacy Standard. "Standard" data are routine health information; that is, identifiable health information that does not fall into any of the "deniable" categories. "Public-deniable" includes informa-

tion about conditions specifically addressed by state law, such as mental health, HIV/AIDS, abortion, adoption, sexually transmitted diseases, and substance abuse. "Guardian-deniable" is health information that by law can be withheld from a guardian, such as (in some states) information about a teenager's abortion. "Patient-deniable" is information that the patient's primary care physician considers capable of causing harm to the patient were it disclosed to that patient. The HIPAA Privacy Standard recognizes three types of "patient-deniable" information—psychotherapy notes; information compiled for use in a civil, criminal, or administrative action or proceeding; and certain information that is subject to or exempted from the Clinical Laboratory Improvements Amendments (CLIA) of 1988. No data were specifically excluded from the PCASSO system.

The client application is contained in a Java applet that communicates with the PCASSO server over a TCP/IP link. The PCASSO server performs security mediation in accordance with the role-based security policy. A firewall stands behind the PCASSO server to protect the university's information systems, while the PCASSO host sits directly on the Internet. Host hardening and internal firewall functions protect the PCASSO server from external threats to its data and services. The architecture combines a protected Java client, a secure communication protocol, a trusted application server, and secure administration services to enable authorized persons to view specific information in the clinical data repository, or to perform privileged actions such as relabeling data or assigning and revoking access rights. All actions on the PCASSO host are audited.

Because this paper reports the results of our evaluation of the model with our test users, we describe here the experience of using the PCASSO system. The user logs in using multi-factor authentication involving a password, a challenge-response token, and a public–private key pair. The graphical image of a keyboard is used to enter all security-critical information, such as the user's password and patients' names. The user starts a Web browser (Netscape Navigator or Microsoft Internet Explorer) and enters the PCASSO URL, which retrieves a file containing the Java code for the PCASSO graphical user interface and displays the login screen shown in Figure 1.

The user enters her user ID and password through the graphical keyboard, after which the client asks the user to insert a personal read-only, encrypted diskette containing her private key. The client and server use their respective public–private key pairs to

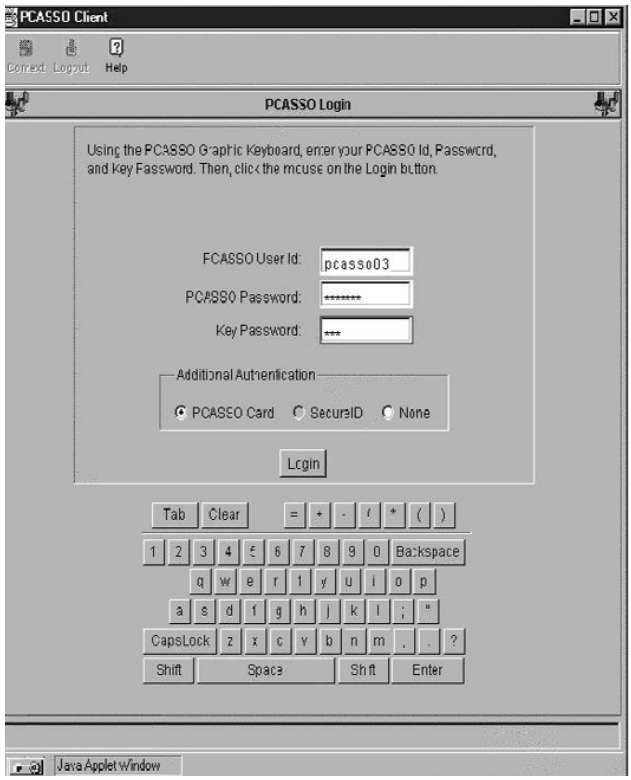


**Figure 1** PCASSO login screen.

mutually authenticate each other ("handshake"), and the application notifies the user that a secure connection has been established. The user then is asked to input the next character string that appears on her "PCASSO card," a laminated card containing random numbers that are synchronized with a corresponding list stored on the server. The PCASSO model system provides all the security services required by the HIPAA security standard and the HCFA Internet security policy.*

Following authentication, a screen customized for the user's context (patient or provider) is displayed. If the user is both a patient and a provider, she is asked to select which context she wants to use for the current session. The server receives the user's requests, determines what data she can see and what actions she may perform, and returns the results. If the user is a provider, the server prompts her to select a patient. She may type either a name or a non-zero character string to return a list of patients whose names begin with that string and for whom she has

*For a detailed description of the PCASSO architecture and operations concept, see Baker.[17]

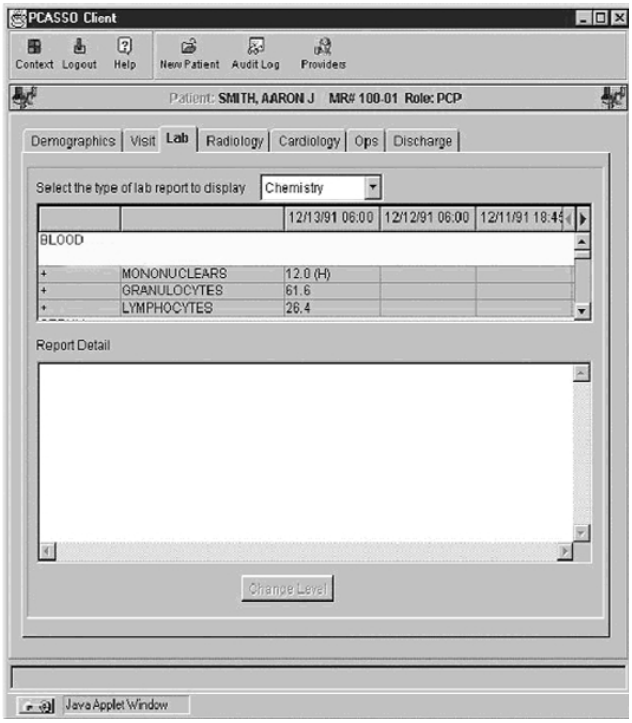


**Figure 2** Sample results screen.

been authorized a provider role. A results screen for laboratory data is shown in Figure 2.

At the completion of each usage session, users are prompted but not required to fill out a user response form regarding the just-completed session, which is shown in Figure 3. Feedback from the response forms was used to assess user perceptions and behaviors.

### Evaluation Criteria

The PCASSO system was evaluated using the same criteria used by the Food and Drug Administration to evaluate medial devices—Is it safe and is it effective? Safety was judged using both qualitative and quantitative measures. Qualitative measures were evaluated using feedback from users regarding their perceptions of the security provided by the PCASSO system. Data sources for quantitative evaluation included access logs and system penetration activities. The system is instrumented to detect a wide variety of attempts to intrude or misuse the system, including unauthorized login attempts; attempts to modify data; and misuse of the "emergency" role. System penetrations were measured both through formal penetration testing exercises ("white hat" hacking) and ad hoc penetration attempts from the Internet at large. Effectiveness was judged using feedback from samples of both providers and patients.

### Pilot Deployment

The model system was first released as a pilot to credentialed UCSD faculty physicians to judge its safety and efficacy, as well as its suitability for use by patients. A total of 210 faculty physicians were enrolled as users during the pilot. At the time of the pilot deployment, the system contained demographic, clinical laboratory, radiology, and dictated transcribed reports for 178,000 patients for whom care was provided in the UCSD Healthcare network, dating from mid 1998. The clinical data repository was continuously updated with copies of new data sent by the operational UCSD clinical information system. Although the PCASSO system provided neither the "open" access nor the features of the internal clinical information systems interface at UCSD, the benefit to physicians was the ability to securely access their patients' data from any Internet-connected PC, essentially from anywhere in the world. The data acquired from the pilot deployment to physicians showed the system to be operating according to its security design principles, without any penetrations, intrusions, or other breeches of information security and confidentiality being detected.

### Full Deployment

Using the results of the system usage by providers as an indicator of system safety and efficacy, application was made to the UCSD IRB in May 1999 to open the system for use by patients. Patients were eligible to participate if the following conditions were met:

- They were active UCSD Healthcare patients (i.e., had at least one clinic visit or hospitalization within the previous year)
- They had pre-existing Internet access, and a compatible computer (the project did not support the costs of computers or online access for participants)
- Their primary care physician agreed to their participation and co-signed the informed consent document acknowledging the patient's participation in the project and its implications.

Patients who met these criteria completed a computer use and demographics survey, and a user account was created for them by the PCASSO user support staff. The support staff included members of the UCSD biomedical library staff who have extensive experience in helping persons use PC technology and find answers to health-related questions from a variety of sources. PCASSO's multiple complementary

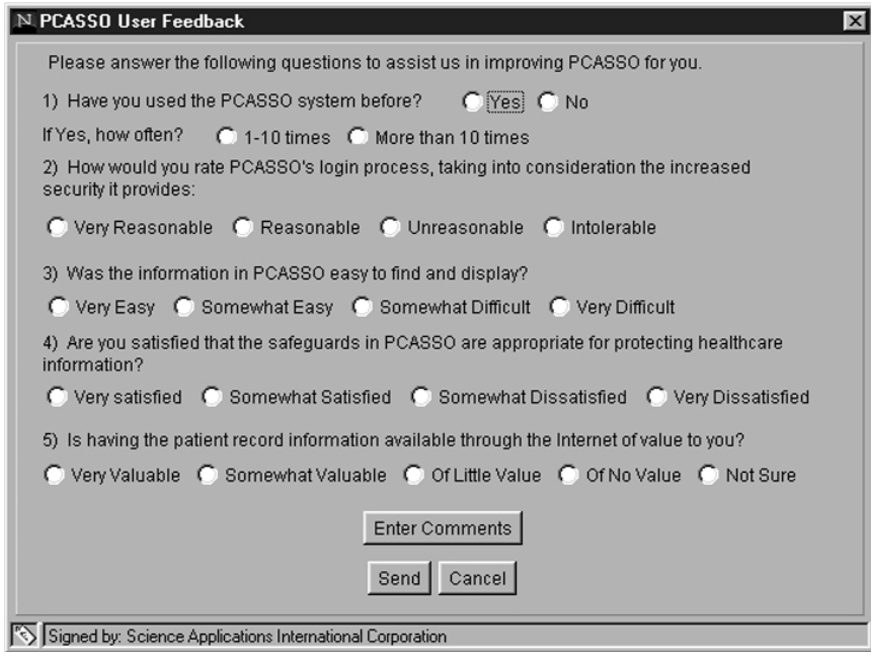


**Figure 3** Feedback form.

security mechanisms ensured that patients could view only their own medical data, excluding any data that the patient's primary care provider had specifically labeled "patient-deniable."†

Each new user received a security diskette containing that user's private key, a user guide with a tutorial on how to use the system, and a PCASSO card, as described above. New users were also given a toll-free number to call in case they had either technical or medical questions that arose as a result of using the system. This number connected them to the PCASSO support staff at the UCSD biomedical library. The library support staff were expected to answer technical questions related to use of the system, and a triage protocol was used to handle inquiries related to medical information received by patients.

### Human Subjects Research Issues

As noted above, the PCASSO project required review by the UCSD IRB before patients could be involved in the research. The IRB required clarification of several issues before approving participation by patients, and may have been sensitized to issues of health information privacy by our providing a background description of Internet-associated security threats. These issues and our approaches to dealing with them are presented here because we believe they are a harbinger of concerns that will arise in health care organizations generally as a result of HIPAA-mandated access to medical records by patients and the increasing use of electronic medical records.

Human subject protection concerns focused on three areas—unauthorized access to information by persons other than the patient; the effect of patients' seeing startling or poorly understood information; and the effect of patient access to records on the record-keeping behavior of providers. These issues and our approach to dealing with them are described below.

The IRB was concerned about the scenario of theft of information access, such as by a family member of a patient participating in the clinical trial of the system. The response to this concern noted that electronic information security requires that access be granted only after user authentication (i.e., proving that one is who he claims to be) that is based on some combination of "something the user knows" (e.g., password), "something the user has" (e.g., token), and "something the user is" (e.g., fingerprint).

PCASSO uses something the user knows (user ID and password pair) and something the user has (an encrypted, read-only security diskette and a PCASSO key). Also, PCASSO account creation involves physical validation of the user's identity by a trusted party (i.e., physician). Thus, although it is possible to give away one's identity, this would require that the authorized PCASSO user actually train a family member in how to assume his identity, as well as give the family member

†The HIPAA Privacy Standards do not allow for denial of patient access to any of their medical information.

the necessary security diskette and PCASSO card. PCASSO does not allow information to be saved to disk on the user's PC and does not allow information to be copied to other applications. Thus, the risk of theft is substantially lower than the risk that would be associated, for example, with paper health records maintained by the patient or with a password-protected Web site for which the patient had saved the password locally via their Web browser.

Several IRB questions related to the potential psychological harm of startling or poorly understood information. Because the PCASSO system makes information available to providers and patients simultaneously, the scenario of a patient's gaining access to a particular laboratory result or dictated note before his providers see it is a genuine concern. However, the content the patient would view is identical to the information that he would receive if he requested a photocopy of his clinical records. The issue is further clouded by the fact that what patients may find startling is "in the eye of the beholder" and cannot be predicted a priori, just as medical emergencies are generally defined by patients and not by providers.

The IRB asked what would happen if the record contained a new diagnosis of a disease such as cancer and, because of timing or scheduling difficulties, the physician had not had an opportunity to get back to the patient personally before the patient read it on the computer. The PCASSO team called this the "out-of-the-blue diagnosis" scenario, in which a completely unexpected result appears and the physician and patient have had no prior discussion of possible outcomes.

An analysis of this scenario reveals that definitive diagnoses virtually always follow a specific test or procedure ordered by a provider, rather than a screening test. For example, a routine chest x-ray report might note a previously unreported mass, and a routine complete blood count may reveal a high white cell count, but the initial reports of these abnormalities do not state conclusive diagnoses, and uniformly comment on the need for further evaluation. Cancer requires a tissue diagnosis and a procedure to obtain that tissue.

The PCASSO project relies on the premise that consent for diagnostic procedures has included a discussion of the reasons for those procedures. Stated otherwise, if a patient could truly say, "I never knew they wanted to do a biopsy because one of the possibilities was that I might have cancer," then both PCASSO and the patient would fall victim to a prior failure to obtain fully informed consent for clinical care.

To address the concerns of the IRB, the PCASSO project incorporated the following four elements into the system design:

- The PCASSO system filters those results transactions labeled "pending" or "interim" and displays only final results. Subsequent amendments and revised results replace any clinical data found to be in error.
- The project's informed consent language was amended to read:

  > The information you will be able to access via the PCASSO system is technical and contained in systems that were originally designed for trained health professionals' use only. As a result, there is a possibility that you will be exposed to information that you do not understand or find startling. PCASSO is not intended to place on you the burden of interpreting your medical record, nor to cause you to act on the information received without first discussing it with your physician. One of the risks associated with this study is that "a little knowledge is a dangerous thing." By agreeing to participate, you agree to contact your physician to help resolve any questions or problems that may arise as a result of viewing your medical data online. If you have difficulty contacting your physician, you may contact the PCASSO project staff, who will assist you in contacting your physician.

- A toll-free phone "hotline" was established and a formal triage mechanism created for inquiries from distraught patients. The primary user support for the project was provided by the UCSD biomedical library and staffed by a librarian with extensive experience in assisting patients with cancer and other serious diseases. The triage protocol included contacting a patient's primary care physician to make the physician aware of patient concerns, and immediate referral to the psychiatry service crisis intervention team if circumstances warranted.
- By study design, all such instances would be considered "information toxicity" and reported to the IRB as adverse events. The project staff looked to the IRB as a pro-active data and safety monitoring group that could help represent the balance of interests of participants and UCSD Healthcare providers.

The IRB also questioned whether physicians' knowing that their patients would have computer access to their health records would discourage the physicians from recording candid and detailed observations and impressions. The project response to this issue was that physicians create their records with the knowledge that those records may be subject to review in

the future for a variety of purposes, including quality assurance, risk management, and legal inquiry. In addition, patients can and do request copies of their paper-based records, including provider notes. Indeed, the PCASSO security technology enables providers to raise the sensitivity level of specific information in the record to the "patient-deniable" sensitivity level, which enables other authorized providers to view the information but removes it from view by the patient. Individual results and reports can also be given this label via a set of rules used by the system's import function. For example, one loading rule stated that all notes originating from the psychiatry department would default to the patient-deniable category.

The IRB required that the project plan be reviewed by the risk management office of the UCSD Medical Center and by the Office of General Counsel of the University of California. Among these advisors, the general consensus was that the benefits of providing patients with online access to medical records far outweighed the risks. Given the technical capabilities provided by a high-assurance system like PCASSO and the growing ubiquity of the Internet, it could be argued that a liability might more likely derive from delaying patient access to information to which they are entitled than from providing it to them under the terms of consent used in the project. The advisors also noted that PCASSO could reduce the institution's liability by virtually ensuring that results would receive expeditious review by someone. Legal counsel also emphasized the imperative to direct patients to contact their physicians to discuss the specific implications of test results and other information viewed using the system.

## Results

The prototype PCASSO system was installed at UCSD for 12 months. During that time, our audit detected a number of attempted intrusions, but to our knowledge the system was never penetrated. In March 1999, the operational system was subjected to an intense and comprehensive simulated attack by a computer security "penetration team" from a division of SAIC (Science Applications International Corp., San Diego, California) that was not involved in the PCASSO development. This team used more than 300 "hacker" tools and penetration techniques acquired from commercial sources, obtained from the hacker "underground," or developed by the company. The system passed this test flawlessly; results of this testing have been published.[11]

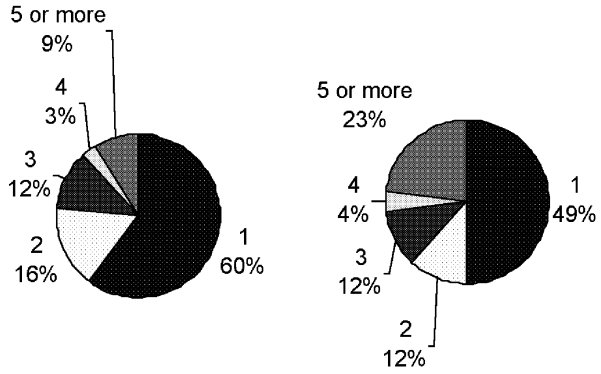


**Figure 4** Comparison of numbers of sessions. *Left*, number of provider sessions; *right*, number of patient sessions.

A total of 216 physicians and 41 patients were enrolled as users of the system, of whom 68 physicians and 26 patients logged in one or more times. At the time of the full trial, the PCASSO clinical data repository contained clinical data for more than 178,000 patients. The typical physician enrollee was male (78 percent) and had good computer skills (53 percent) and good knowledge of the Internet (48 percent). The typical patient enrollee was female (73 percent), was well educated (71 percent with college degree), and had excellent computer skills (49 percent) and excellent Internet knowledge (54 percent). The vast majority of enrollees had well-equipped PCs, with 47 percent having Pentium II or Pentium Pro processors with clock speeds of 90 MHz or higher (77 percent) and at least 64 MB of RAM (57 percent).

A considerably larger percentage of patient enrollees actually used the system than did physicians—26 of the patient enrollees (61 percent) compared with 68 physicians (31 percent). Of those who used the system, more patients logged in at least five times (23 percent) than did physicians (9 percent), despite the fact that most of the physicians had access to the system for at least 10 months, whereas PCASSO was accessible to patients for only 6 months. An informal sampling of patients who enrolled but did not use the system revealed that the most common reason for not accessing the system was that they had not had a recent clinic visit. The distribution of the numbers of sessions for physicians and patients is shown in Figure 4.

The user feedback form asked for feedback in several areas—reasonableness of the PCASSO security features, effectiveness of the system, ease of use, and usefulness of the data. As described earlier, logging


**Figure 5** Perceptions of PCASSO login process. *Dark columns,* physicians' ratings; *light columns,* patients' ratings.

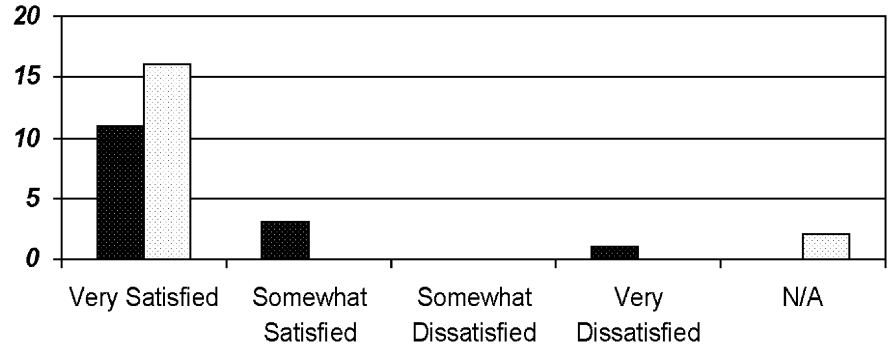


**Figure 6** Perceptions of PCASSO safeguards. *Dark columns,* physicians' ratings; *light columns,* patients' ratings.

into the PCASSO system is a multi-step process requiring the use of a user ID, a password, a diskette, and a PCASSO card. This multi-step process is designed to provide a high level of assurance that users are indeed who they claim to be and that they are authorized to use the system.

Patients and physicians judged this process quite differently, as shown in Figure 5. Sixty-eight percent of the patients who provided feedback (18 users) considered this process "very reasonable," whereas none of the physicians who provided feedback (15 users) considered it so. Indeed, fully 88 percent of the patients who provided feedback rated the login process either "very reasonable" or "reasonable," 11 percent rated it "not applicable," and none considered it either "unreasonable" or "intolerable."

Although 60 percent of the physicians who provided feedback rated it "reasonable," the remainder of the physicians who provided feedback rated it either "unreasonable" (20 percent) or "intolerable" (20 percent). The differences between patient and physician ratings of the acceptance of the login process were statistically significant, with a two-tailed $P$ value of less than 0.0001 as measured by the Mann-Whitney test.

Despite the negative perceptions of the physicians, when asked to rate their degree of satisfaction with the PCASSO safeguards, both physicians and patients said they were "very satisfied." Figure 6 shows a comparison of the physicians' and patients' ratings of the PCASSO safeguards.

With respect to effectiveness, we also asked the users to rate the overall value of having records available to them over the Internet. As shown in Figure 7, a majority of both physicians and patients rated the value as "very high." No one said they found no value in having medical records available, and only one physician rated Internet accessibility of "little value."

Users were also given the opportunity to provide free-text feedback. A number of physicians and patients commented that some specific information they were looking for was not available. This resulted from several circumstances. First, the PCASSO clinical data repository was populated with real-time data sent from active clinical systems; it was not preloaded with data recorded before PCASSO was installed. Second, some data types (e.g., urinalysis serology) were simply not implemented in the model system. Finally, some data may not yet have been sent to PCASSO at the time a user logged in.

The primary comment from the physicians was that the role-based access controls did not allow them to view all the data in the system, as they currently can using the operational clinical system. Also, some security features, such as the multi-step challenge-

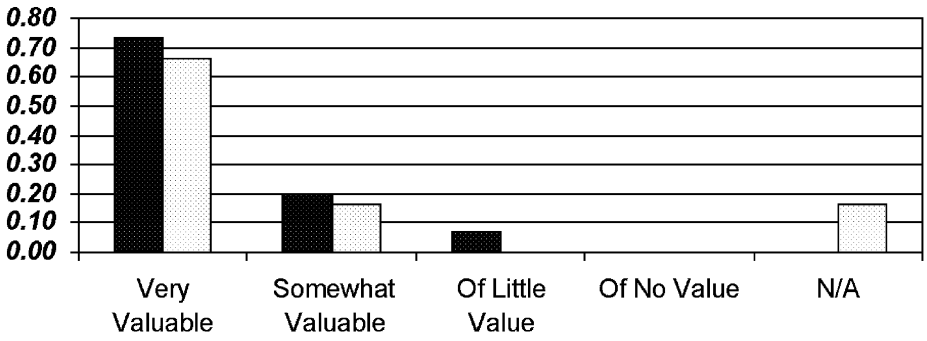


**Figure 7** Perceptions of value of having records accessible on the Internet. *Dark columns,* physicians' ratings; *light columns,* patients' ratings.

response user authentication and use of a graphical keyboard in place of the physical keyboard, generated a substantial number of negative reactions.

Some comments from patients suggested that the IRB's initial concern that patients might overreact or panic if they saw results without having their physicians there to explain them was not an issue in this group of users, although one patient asked for a "key to understand the notation in my lab report." Other comments simply expressed appreciation for having the information available:

> I was at the lab this morning and some results are posted already…very impressed!!
>
> It was great to be able to read my lab results, as my physician has not reported them to me.

We also saw indications that PCASSO influenced patients' behaviors and assisted clinicians in providing care. One user said that he or she "caught the lab doing the wrong test and had it corrected." Another noted that his or her lab results were not yet in the system, so he or she would "wait a few days before I call the office."

We received positive comments from both physicians and patients. Here is a sampling:

> As a demonstration of "SSO" part of the acronym, it seems very secure—certainly much more so than most e-commerce transactions (including stock trades) I've done. It's incredibly handy to have this stuff available on the Internet. Nice work. (From a physician)
>
> Thank you for this "peek" into our own medical records. So often patients seem to feel at the mercy of the HMOs, and at least this may alleviate some of that distrust.
>
> Love this program and it really is super easy to use! Did notice that I have 3 PCPs, when actually two of them are specialists. …Nice to get to read reports of special tests. Thanks!
>
> As one who has always been involved in my health care decisions, I value that I have access to this information. Great system. I find it very user friendly and feel very confident that my privacy is maintained at all times. Thank you for allowing me the opportunity to use it.

## Discussion and Conclusions

The qualitative data we collected from our users and the quantitative audit and penetration data revealed that the PCASSO system is both perceived to be safe and is safe. Both physicians and patients gave PCASSO very high ratings on its safety, and the system has continually resisted attack. One unsolicited comment came to us from a person who approached one of the investigators following a talk about the project, handed the investigator a business card, and identified himself as a "professional hacker." He said that he had been targeting the PCASSO server for some months and to that point had been unsuccessful in penetrating it. We were gratified by his observation that "you guys really know what you're doing."

However, this safety has come with a price in usability. The PCASSO system clearly is more difficult to use than the systems to which most people are accustomed. Our data suggest that, for patients, some "challenge" is acceptable and may even have value, in that it contributes to the perception of safety. However, some features, while contributing to PCASSO 's safety, may be overly burdensome, particularly for providers, to the point of affecting PCASSO 's effectiveness. Our data suggest that our patients may value security over convenience, whereas our providers' values may be quite the reverse.

A clear majority of our users found value in having patient information accessible over the Internet. But that effectiveness is moderated by a user experience that may discourage its use. Our findings suggest that security features need to be flexible and configurable, based on the needs and expectations of users and the risks an enterprise is willing to assume.

*Table 1* ■

PCASSO meets HIPAA's Requirements for Technical Security Services to Guard Data, Integrity, Confidentiality, and Availability

| Requirement | PCASSO Model |
|---|---|
| Emergency access | Yes |
| Context-based, role-based, or user-based access control | Role-based |
| Encryption over public networks | Yes |
| Audit controls | Yes |
| Role-based or user-based authorization control | Role-based |
| Data authentication | Encryption ensures integrity of data passed over the Internet; importer rejects malformed messages |
| Automatic logoff | Yes |
| Unique user identification | Yes |
| Biometric, password, PIN, telephone callback, or token | Password and token |

*Table 2* ■

PCASSO meets HIPAA's Requirements for Technical Security Mechanisms to Guard Against Unauthorized Access to Data That is Transmitted over a Communication Network

| Requirement | PCASSO Model |
|---|---|
| Integrity controls | Encryption protects integrity of data; label-based access control protects integrity of executable code |
| Message authentication | Encryption authenticates message integrity; no MAC or digital signature |
| Access controls or encryption | Access controls and encryption |
| Alarm | Server senses loss of client |
| Audit trail | Yes |
| Entity authentication | Both server and client are authenticated |
| Event reporting | Detection/reporting of intrusion attempts and misuse of "emergency" role |

We are often asked whether the PCASSO model is "HIPAA compliant." Our first response is to observe that the final HIPAA Security Standard has not yet been released. However, evaluating PCASSO against the final Privacy Standard, we observe that PCASSO empowers patients consistent with the letter and spirit of the standard, including support for its "minimum necessary" mandate. Evaluating PCASSO against the August 1998 Security Standards Proposed Rule, we find that PCASSO contains all the features specified for technical services and mechanisms, as shown in Tables 1 and 2.

Through our experience in building and evaluating the PCASSO model, we have shown that a system can be built that is strong enough to provide safe access to highly sensitive personal health information over the Internet. However, building systems that meet both patients' expectations for privacy and safety and their providers' expectations for convenience and usability remains a substantial challenge. Work to achieve these goals is currently under way.

*References* ■


1. Cimino JJ, Socratous S, Clayton PD. Internet as clinical information system: application development using the World Wide Web. J Am Med Inform Assoc. 1995;2(5):273–83.
2. Chute CC, Crowson DL, Buntrock JD. Medical information retrieval and WWW browsers at Mayo. Proc Annu Symp Comput Appl Med Care. 1995:903–7.
3. Jagannathan V, Reddy YV, Srinivas K, et al. An overview of the CERC ARTEMIS project. Proc Annu Symp Comput Appl Med Care. 1995:12–6.
4. Kahn CE, Bell DS. WebSTAR: platform-independent structured reporting using World Wide Web technology. In Hripcsak G. ed. Proc AMIA Spring Congress. 1995:86.
5. Masys DR, Baker DB. Patient-centered access to secure systems online (PCASSO): a secure approach to clinical data access via the World Wide Web. Proc AMIA Annu Fall Symp. 1997:340–3.
6. Baker D, Barnhart R, Buss T. PCASSO: applying and extending state-of-the-art security in the healthcare domain. Presented at: 13th Annual Computer Security Applications Conference; San Diego, California; Dec 12, 1997. Available at http://medicine.ucsd.edu/pcasso/.
7. Masys DR, Baker DB, Barnhart R, Buss T. PCASSO: A secure architecture for access to clinical data via the Internet. Medinfo. 1998;9 pt 2:1130–4.
8. Masys DR, Baker DB. Protecting clinical data on Web client computers: the PCASSO approach. Proc AMIA Symp. 1998:366–70.
9. Baker DB, Masys DR. PCASSO: a design for secure communication of personal health information via the internet. Int J Med Inf. 1999;54(2):97–104.
10. Baker DB, Masys DR. Assurance: the power behind PCASSO security. Proc AMIA Symp. 1999:666–70.
11. Health Care Financing Administration Internet Security Policy. Nov 24, 1998. HCFA Web site. Available at: http://www.hcfa.gov/security/isecplcy.htm
12. Pritts JJ, Goldman J, Hudson Z, Berenson A, Hadley E. The

State of Health Privacy: An Uneven Terrain. Washington, DC: Health Privacy Project, Georgetown University, 1999:22.
13. National Committee on Vital and Health Statistics. Uniform Data Standards for Patient Medical Record Information. Report to Secretary of U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act (HIPAA) of 1996. Washington, DC: DHHS, 2000.
14. Department of Health and Human Services. Standards for Privacy of Individually Identifiable Health Information. Billing Code 4150-04M. Federal Register, Dec 28, 2000, pp 82461–82829 (45 CFR parts 160-164).
15. Department of Health and Human Services. Security and Electronic Signature Standards: Proposed Rule. Federal Register, Aug 12, 1998, pp 43241–43280 (45 CFR part 142).
16. California Health and Safety Code, Section 123100. Available at: http://www.leginfo.ca.gov/calaw.html
17. Baker DB. PCASSO: a model for safe use of the Internet in health care. J AHIMA. 2000;71(3):33–6.