

# Giving Patients Access to Their Medical Records Via the Internet: The PCASSO Experience

*Daniel Masys, MD<sup>1</sup>, Dixie Baker, PhD<sup>2</sup>, Amy Butros, MLS<sup>3</sup>, Kevin E. Cowles<sup>3</sup>*

*<sup>1</sup>School of Medicine, University of California, San Diego, <sup>2</sup>Science Applications International Corporation, <sup>3</sup>Biomedical Library, University of California, San Diego  
dmasys@ucsd.edu*

The Patient-Centered Access to Secure Systems Online (PCASSO) project is designed to apply state-of-the-art security to the communication of clinical data over the Internet. At the time the project began, there existed several prototype, Web-based clinical data systems<sup>1-5</sup>; however, these were explicitly designed to serve only health professionals, and most used security “firewalls” to filter queries originating from outside the 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 communications, 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 and control his or her own health data.

The PCASSO security model explicitly recognizes the rights and responsibilities of providers and their patients and implements those rights and responsibilities via access, confidentiality, integrity, and accountability controls that are compatible with public data networks such as the Internet. The technical details of the system design—including overall architecture<sup>6</sup>, security model and concept of operations<sup>7</sup>, approach to overcoming client-side vulnerabilities<sup>8-10</sup>, and methods for attaining high assurance of correct operations<sup>11</sup>—have been published.

The system was released for use by credentialed University of California, San

Diego (UCSD) faculty physicians in January 1999 and enrolled 216 faculty physicians as users, 68 of whom (31 percent) used the system one or more times. At the time of initial deployment, the system contained demographic, clinical laboratory, radiology, and dictated transcribed reports on 174,000 patients cared for within the UCSD Healthcare network since mid-1998, and it was continuously updated with copies of new data sent to the operational UCSD clinical information system. The benefit of PCASSO for providers is that they may use the system to securely access data on their UCSD patients from any Internet-connected PC anywhere in the world. In March 1999 the operational system was subjected to an intense and comprehensive attack by a computer security “tiger team” of Science Applications International Corporation (from a division not related to the development team) using more than 300 “hacker” tools and penetration techniques developed by and for the National Security Agency. The system passed this test without successful intrusion or interruption of service<sup>11</sup>.

Using the results of the system usage by providers as an indicator of system safety and efficacy, application was made to the UCSD Institutional Review Board (IRB) in May 1999 to open the system for use by patients. Human subjects concerns raised by the IRB 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. The IRB also required legal review and approval of the project by attorneys representing the UCSD

Healthcare Risk Management and General Counsel of the University of California. The project employs several mechanisms to address issues related to potential “information toxicity,” including special informed consent language, cosignature of consent documents by primary care physicians, and a formal triage mechanism for distraught participants.

The project enrolled 56 patients during its initial clinical trial, 33 of whom (59 percent) used the system one or more times. To date, no adverse events have occurred. The system performed as designed, with no unauthorized information access or intrusions. User support was provided by a systems administrator and outreach librarian of the UCSD Biomedical Library.

Online exit surveys were used to assess perceptions of the security, usability, and value of information received. As shown in Table 1, 6 of the 15 providers (40 percent) who completed the survey rated the usability of the system as either unreasonable or intolerable due to the complexity of the secure login and other security features, such as inability to use the workstation keyboard for data entry. In contrast, all 16 of the patients who completed the survey rated the security features and usability as either reasonable or very reasonable.

Table 1. User Perceptions of PCASSO Security

Rating	Providers N=15	Patients N=16
Very reasonable	0	12 (75%)
Reasonable	9 (60%)	4 (25%)
Unreasonable	3 (20%)	0
Intolerable	3 (20%)	0

By providing immediate online access to laboratory results, radiology and special procedures reports, and dictated provider notes, PCASSO has served as a harbinger of a “Health Insurance Portability and Accountability Act-enabled”<sup>12</sup> era of

electronic access by patients to their medical records. The project has also demonstrated the value of support by medical librarians in assisting patients to access their medical records online and understand the content of those records.

#### ACKNOWLEDGMENT

This project has been funded in part with Federal funds from the National Library of Medicine under Contract No. N01-LM-6-3537-00.

#### REFERENCES

1. Cimino JJ, Socratous SA, Clayton PD. Internet as clinical information system: application development using the World Wide Web. *J Am Med Inform Assoc* 1995;2(5):273-283.
2. Chute CG, Crowson DL, Buntrock JD. Medical information retrieval and WWW browsers at Mayo. In: Gardner RM, ed. *Proc Annu Symp Comput Appl Med Care* 1995;903-907.
3. Jagannathan V, Reddy YV, Srinivas K, Karinthe R, Shank R, Reddy S, Almasi G, Davis T, Raman R, Qiu S, et al. An overview of the CERC ARTEMIS Project. In: Gardner RM, ed. *Proc Annu Symp Comput Appl Med Care* 1995;12-16.
4. Kahn CE, Bell DS. WebSTAR: Platform-independent structured reporting using World Wide Web technology. In: Hripcsak G, ed. *Proc Spring Congr AMIA* 1995;86.
5. Kohane IS, Greenspun P, Fackler J, Szolovits P. W3-EMRS: access to multi-institutional electronic medical records via the World Wide Web. In: Hripcsak G, ed. *Proc Spring Congr AMIA* 1995;86.
6. Masys DR, Baker DB: Patient-Centered Access to Secure Systems Online (PCASSO): a secure approach to clinical data access via the World Wide Web. *J Am Med Inform Assoc* 1997;340-343.
7. Baker D, Barnhart R, Buss T. PCASSO: applying and extending state-of-the-art security in the healthcare domain. *Proc Annu Comput Secur Appl Conf*. Full text available at <http://medicine.ucsd.edu/pcasso/publications>.
8. Masys DR, Baker DB, Barnhart R, Buss T. PCASSO: a secure architecture for access to clinical data via the Internet. *Proc Am Med Inform Assoc* 1998.

9. Masys DR, Baker DB. Protecting clinical data on Web client computers: the PCASSO approach. *J Am Med Inform Assoc* 1998;366-370.
10. Baker DB, Masys DR. PCASSO: a design for secure communication of personal health information via the internet. *Int J Med Inform* 1999;54(2):97-104.
11. Baker DB, Masys DR. Assurance: The power behind PCASSO security. *J Am Med Inform Assoc* 1999;666-670.
12. <http://aspe.hhs.gov/admsimp/>