Policy Forum ■

Security versus Access: Trade-offs Are Only Part of the Story

STEVEN SHEA, MD

Security is not sexy, flashy, or hot. The best clinical information systems, the most profitable vendor-provided software packages, and the leaders in medical informatics are not known for system security. These systems, products, and leaders are known for getting information and people together, not keeping them apart. Nor has security been a mainstream concern at SCAMC. In 1990, 1991, and 1992 there were 669 articles published in the *Proceedings*, but of these only four were concerned with privacy or security. Although security and security specialists have been part of the technology for many years, they have only recently moved to the forefront of medical informatics.

To what can this new level of attention be attributed? Primarily to three factors: the success of medical informatics in building large-scale systems in which vast amounts of data are shared across applications and are readily available to a great many users; the use of networks to achieve these successes with concomitant emergence of new kinds of security problems; and the technical feasibility of the computerized patient record within the next decade coupled with the realization that the security concerns of patients and physicians could slow or prevent the realization of this potential. In short, the growing concern with security is due to our own success.

What are the risks posed by violations of data security and information confidentiality?

- Loss of privacy.
- Personal or professional damage, such as loss of affection or respect of family members or loss of employment or insurance, if certain illnesses become known.
- Harrassment or blackmail.
- Lawsuits, particularly against those with legal and fiduciary responsibility to maintain medical confidentiality.
- Social control. Within the lives of our parents and of some of us, we have examples that range from discrimination to internment, eugenics, and even genocide. The risk of social misuse of medical information arises in part from the potential for linkage of databases across domains, such as between medicine and law enforcement or credit rating.

There are serious risks. Therefore, we must take concerns with confidentiality and security seriously, and we must act to address them. Thus, the first important conclusion is that acceptance of reduced security as a trade-off for improved medical information management is not a useful or responsive posture.

Where are the exposures? Any list is necessarily incomplete. Five areas are worth highlighting:

- Lack of institutional policies and procedures.
- The widespread use of networks to transfer data.
- Downloaded data in nonsecure servers.
- Lack of robust authentication and authorization procedures that can span heterogeneous, networked systems.
- Lack of resources.

Figure 1 shows the architecture of a typical hospital or academic medical center information system. In most institutions, policies indicating what kinds of security must be present in such information systems, and procedures for dealing with violations, are incomplete. Authentication messages and data are

Affiliation of the author: Division of General Medicine and Center for Medical Informatics, Columbia University, New York, NY.

Correspondence and reprints: Steven Shea, MD, Columbia University, PH8 West, 622 West 168th Street, New York, NY 10032.

Received for publication: 3/15/94; accepted for publication: 3/18/94.

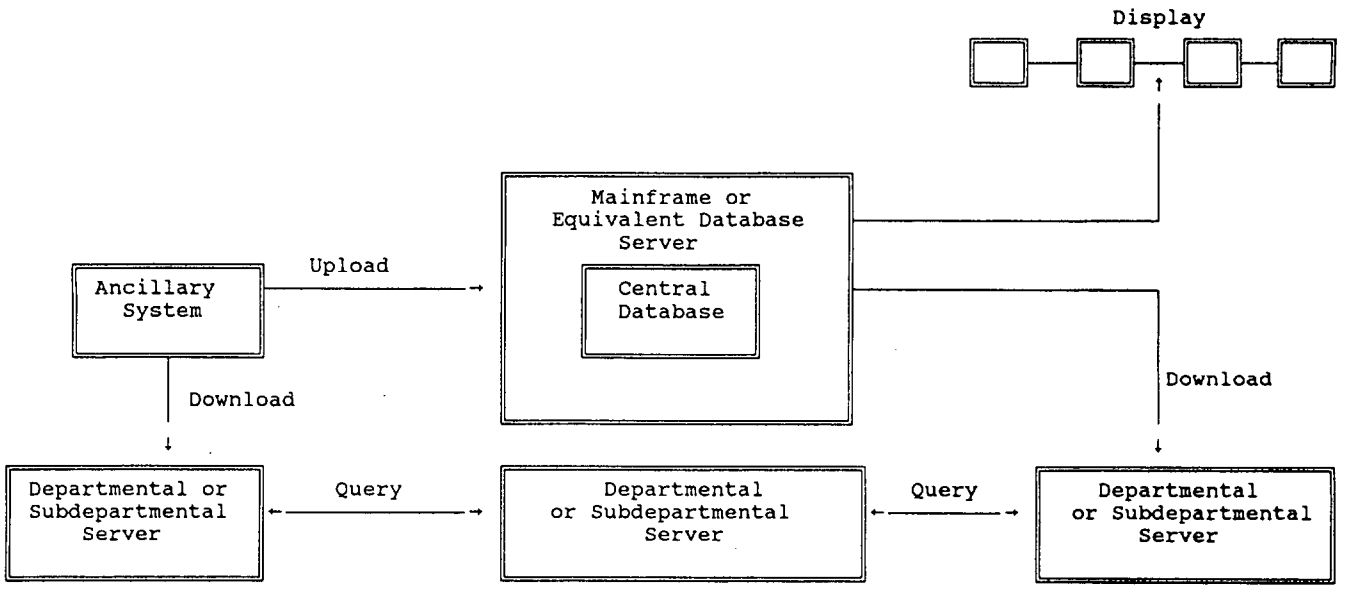

Figure 1 The architecture of a typical hospital or academic center information system.

generally transferred in unencrypted form. Data are routinely uploaded from and downloaded into departmental or ancillary servers that are outside the management or control of institutional administrators. Authentication schemes are usually specific to servers and network management software, without central management. Access to the network may be possible by remote dial-in, with remote access to specific servers possible using server-specific authentication procedures, again outside central management. Generally, there are no standards for authentication schemas for servers attached to the network. Finally, few resources are allocated to this problem, since it is the sort of problem where only the failures, not the successes, are noticed.

What approaches can we take to reduce risk?

- Policies, procedures, and laws and their enforcement all need to develop alongside capabilities for the computer-based record.
- Encryption provides an important layer of protection. Because of cost, encryption probably has a selective role now and will continue to have such a role in the near future (e.g., encryption of authentication messages).
- Control and management of data distribution, particularly downloading, is primarily an administrative issue that can be addressed now.
- Authentication and authorization standards for networks and for servers that receive downloaded data are achievable, once the necessary institutional policies are in place.
- Audit trails are a potentially useful method. Many hospitals that employ audit techniques have anecdotes about their utility, but systematic research on how to process the huge amounts of data and what the true effects are, both as a deterrent and as an enforcement tool, remains to be done.

It is clear from military domains that very high levels of data security can be achieved. While the medical domain differs in many important ways, the transfer of some of this technology may have utility as we seek to improve medical data security.

Several conclusions may be drawn. First, current levels of data security are probably too low and are often insufficient to ease the legitimate concerns of thoughtful people. Second, improved security is attainable through a combination of policy development, administrative organization, and technology development or transfer. Finally, adequate security is a requirement of the computerized patient record, and inadequate security—or the perception of inadequate security—will slow the development and impede the deployment of this potentially very beneficial medical technology. Data security should be viewed as an essential part of the task of building the computerized patient record, not as a trade-off.