For the Record: Protecting Electronic Health Information

Public Briefing
March 5, 1997

OPENING STATEMENT

Paul D. Clayton

Director of Clinical Information Services,
Columbia Presbyterian Medical Center;
Professor and Chair,
Department of Medical Informatics, Columbia University

and

Chair, Committee on Maintaining Privacy and Security in
Health Care Applications of the
National Information Infrastructure

Computer Science and Telecommunications Board
National Research Council

Good morning and thank you for your interest in privacy and security of electronic health information.

Information technology is a critical and powerful contributor to ongoing efforts to improve the quality of health care and lower its costs. Hospitals are developing electronic medical records. Health care organizations are linking facilities, physicians, and clinics electronically over private information networks. People can now enroll in health-benefits programs over the Internet. Information technology is facilitating research into the nature and causes of disease. And someday, doctors will have all the relevant data available and needed to provide cost-effective health care for their patients.

At the same time, new questions arise about the privacy and security of patient information. How can health records be protected if they are stored in an electronic

format — a format that allows information to be sent over expanding telecommunications networks? How can computer systems used in health care be protected against unauthorized attempts to access, alter, or delete patient information? How can patient files be protected yet remain accessible when needed for care?

Answering such questions is critical. Patients must be able to trust health care organizations to protect personal information from willful or accidental disclosures. Health care organizations must ensure that unauthorized users won't break into their information systems and change data. And health information must be available to those who need it — when they need it — for purposes of care.

The National Library of Medicine and the Warren G. Magnuson Clinical Center of the National Institutes of Health, along with the Massachusetts Health Data Consortium, asked the National Research Council to address these issues. The study committee was formed to assess the technical and non-technical mechanisms for protecting electronic health information, to identify other approaches worthy of testing in a health care environment, and to outline promising areas for future research. Its work involved site visits and meetings with many other experts, both to learn about security methods that work and to better understand concerns about privacy and security.

The committee has concluded that electronic health information is essential to improving health care in America. Efforts must focus on finding ways to maintain privacy rather than opposing the use of information technology in health care.

Numerous mechanisms exist today for making systems secure and many can be adopted with reasonable effort. Technical tools can identify and validate the identity of users, limit their access to particular types of information, and keep logs of all accesses to health information. Technologies such as firewalls can stop unauthorized users from remotely accessing information systems, and encryption can protect electronic transfers of information. These technical practices can make information available to those who need it, while keeping it out of the reach of those who don't.

But technical tools are not sufficient to protect health information — whether electronic or paper. A set of *organizational* practices also must be adopted to ensure that those with access to patient health information understand their responsibilities for protecting it, and to assess penalties for those who violate that trust. Policies must be developed to communicate to employees and others the organization's commitment to

protecting health information. Formal structures must be established to formulate, update, implement, and enforce policy.

To encourage such practices, health care organizations need appropriate incentives. To date, these organizations have not had consistent economic and regulatory incentives to strengthen security. Sporadic violations of privacy and security have failed to rally broad interest; and few sanctions exist that compel greater attention to privacy and security. Most organizations face strong pressures to expand the capabilities for access to their health information systems. Those that have put information online are beginning to take protective steps they believe are reasonable and justifiable. However, as the site visits demonstrated, no single organization has adopted the full list of practices we recommend in our report.

Two other factors slow the adoption of security technology in health care. One is a lack of standards that define the types of security mechanisms that health care organizations should demand from vendors of medical information systems. The other is the lack of a mechanism for health care organizations to share information about security breaches that have occurred and practices that are effective in preventing them. The committee hopes its report will inform the crucial work under way at the National Committee for Vital and Health Statistics to develop security standards as part of the response to the Health Insurance Portability and Accountability Act of 1996. Those who collect, analyze, and disseminate health information must continue to develop new standards as the technology, its applications, and the threat to privacy evolve.

Nevertheless, many concerns over patient privacy result not from malicious attackers trying to break into health information systems or from insiders who "leak" information, but from the open and generally legitimate sharing of information among organizations in the health care industry. Most patients would be surprised at the number of organizations that receive information about their health record: their provider, insurer, pharmacist, state public health organizations — perhaps even their employer, life insurance company, or marketing firms. Sometimes only a synopsis of the medical record is shared, other times a report of a particular condition is made. Sometimes names and demographic information are also included.

Sharing of information within the health care industry is largely unregulated and represents a significant concern to privacy advocates and patients alike because it often

occurs without a patient's consent or knowledge. Addressing the privacy concerns posed by these data flows requires continued national debate to help determine how to best balance a patient's privacy interests against other organizations' needs for health information and to ensure accountability for those who have a legitimate use of the data.

Related to these concerns is the current initiative to create a unique health identifier for each patient, provider, employer, and health plan in the health care system, as part of the response to the Health Insurance Portability and Accountability Act. A universal patient identifier has many benefits: The many different records referring to an individual patient across the health care system can be linked more easily for care, payment, administration, or research. But a universal identifier also can be used in ways that adversely affect patient privacy. If information can be linked for legitimate purposes such as collating a complete medical record for a physician, it also may be linked for other purposes that patients might not approve of — and might even allow health records to be linked with records outside the health care system. Such privacy issues must be considered explicitly in any attempt to develop a universal identification system.

Addressing these and other security concerns will require continued attention. Over time, the application of information technology will evolve, and so will its vulnerabilities and the solutions available to protect privacy. Many tools will be developed by the computer security community regardless of the needs of the health care industry. Other tools — such as stronger mechanisms to track accesses to electronic information — might not be developed unless the health care industry calls for them.

The committee believes that adoption of its recommendations will foster continued progress in modernizing the health care industry, while ensuring that privacy and security are maintained.

My colleagues and I will now take your questions. Since this briefing is being recorded, please state your name and affiliation after you receive the portable microphone. Thank you.