the Journal of CONTEMPORARY DENTAL PRACTICE
www.thejcdp.com
Volume 1 Number 4 Fall Issue, 2000

Cyberinfo:
Privacy and Personal Health Data in Cyberspace

James Day, DDS, MEd

Abstract

In this series of articles, the author discusses the potential risks, benefits, and liabilities in using electronic communications and computer-based record keeping for patients' medical data. Article #1 in this series reviews the foundations of privacy for personal information and the current practices of collecting disaggregated private personal and medical data made possible on the Internet by software and hardware configurations.

Keywords: Electronic communications, computer-based medical record, patient medical data, privacy, personal medical data, computer record, medical data, patient care, patient healthcare, data privacy, personal information technology

Introduction

It is always a good idea to maintain an excellent record of patient care. Computer systems support the effective and efficient collection and maintenance of such data. But with the advent of the interconnectivity of the Internet and the effectiveness of data retrieval engines, there is an ever-growing risk of unauthorized "sharing" of patient healthcare data.

This article reviews the foundations for privacy of personal information and the current practices of collecting and assembling separate increments of private personal and medical data made possible on the Internet by software and hardware configurations

The Holy Grail of Privacy

Our culture's concept of privacy spans a wide perspective and is subject to the individual's understanding and in some cases, legal protections. As technology clouds our perspective; the protocols, expectations and practices of conventional wisdom established to protect an individual's privacy become less clear. The advent of computing has forced a quantum change in daily life and the structure and function of the society in which we live. The world of the Internet, with the computing power inherent in its connectivity, radically impacts the individual by allowing the restructuring and redistributing of one's personally associated information. Such "progress" is changing our expectations of personal privacy and quality of life. In reaction to these changes, public opinion and political will are reacting to protect the privacy of the individual.

Imagine, with the advent of radically new computer-based lifestyles, one's data is seamlessly categorized and continually collected and monitored. Previously obscure daily activities and routines are documented and tracked. Travel (electronic airline ticketing, scan-based tolls for parking, roadway use), communications (telephone calling records and e-mail records collected and accessed by ISP's, employers) and credit card use data are all collected electronically. This collection allows instantaneous and selective monitoring of anyone's daily activities. Routine use of this data is not necessarily a troubling idea for the average citizen. But the potential of aggregate data collection by anyone wanting to "put the pieces together" and the ability to effectively and expediently do so, presents new challenges in order to prevent intrusion into the rights of the individual's in the "pursuit of happiness" and to meet public demand for privacy.

Unfortunately, the realities of technology make it possible for online businesses and advertisers to turn the Internet into a realm where activities and habits are monitored and recorded, without consumer knowledge or consent.[1,2] Anything that can be known will be known, and it will be known to a greater degree of precision than was ever thought possible." [3]

With the advent of the "dot-com's" and commercial use, the Internet has become effectively distributed throughout popular culture. Currently the United States has more than 110 million users accessing the Internet for information, commerce, and communication. This is nearly 43% of the world's online population.[4]

The World Wide Web's growth has focused on satisfying the consumer and seeker of information. But programmers and information providers are making covert changes to the system. As the Internet evolves into its third generation of growth, new configurations and functionality, transparent and unknown to the user are being added. The Web is now a "bottom-up" builder and compiler of data and information resources that are both searchable and configurable. The building of powerful analytic information resources based on the aggregation of dispersed individual data defines a new area of growth, prosperity and power for the Internet entrepreneur.[5]

Huge database structures operating under CORBA protocols (Common Object Request Broker Architecture) and XML (Extensible Markup Language) tagged data capabilities facilitate this tracking through the combinatorial power of data system interchange and analysis.

(For more information: http://www3.ncr.com/architecture/occa6/distssvc/dscnt.htm.) Distance, time, and location are spanned in a matter of milliseconds. It is the ability to combine these data elements into a clearly distilled and individually tailored imprint of one's words, actions, deeds, and personal history that begin to loom as a potential demon in the mind of law-abiding citizens.

Framing Legal Protections

In the United States, constitutional law, statutory law, and common-law serve to protect a patient's right to privacy for their personal medical information, or data. Traditionally, the combination of federal and state level implementations of these approaches serve to provide a viable shield for personal data in well-defined domains of information. However, distributed data does not, by nature, reside in one specific location. Electronically based data can be highly dispersed with unlimited instances of collection and use of this data by multiple parties in different places. This fragmentation leads to a complexity in jurisdictional nexus. The rule of federal jurisdictions offers broad and equitable solutions that partially address this complex issue of legal proximity.

Most citizens firmly believe they have the inherent right to choose the lack of intrusion by anyone or any unwanted or unwarranted event in their personal affairs or their day-to-day lives. This belief is premised on the tradition of the United States Constitution and the general expectation of a quality of life with the freedoms that all citizens of the United States assume as their normal and natural state. This protection extends in a fashion under the Fourth and Fifth Amendments of the U.S. Constitution in the restriction of unwarranted government intrusion into the affairs of the citizen. These restrictions are designated to protect the citizen from the government and do not address private or corporate activity in the privacy arena. In fact, some protections offered through the constitution from the government have been diminished by the interpretations of the courts.

The federal government is expected to protect the citizen's privacy as a "civil right." However, the various patchwork of federal legislation that attempts to address the integrity of personal medical information leaves wide gaps in protection. The scope of legislation is often narrowly defined, and the number of exemptions and exceptions to disclosure are often great. The effectiveness and cohesiveness of the resultant legislation lacks the functionality to address the developing needs and desires of citizens to improve privacy protection for medical information.[7]

Claims to advance the application of privacy rights to one's personal medical information have been read into two court cases finding for limited federal protection for specific levels of medical information involving a woman's right to personal choice. In Griswold vs. Connecticut, the court found privacy of medical decision making related to birth control "so personal that they required special safeguarding against any government interference." In Roe vs. Wade protections are also attributed to the physician-patient relationship.[8]

The average citizen views privacy as a right guaranteed and expected under law. In some cases they are correct in their assumptions. This right is generally afforded the individual under common law in four areas of torts:

- Protection from intrusion on the individual's seclusion or solitude
- Protection from the public disclosure of private information
- Protection from framing an individual in a false view which would be highly offensive to the reasonable person
- Nonconsensual use of an individual's identity for private commercial gain [9]

Limitations of disclosure or use of personally identifiable medical information are often best addressed by state law. Medical records have by practice and tradition, been based in both temporal and geographic dimensions. By state statute, Hippocratic Oath, and ethical duty, healthcare professionals have a responsibility to maintain the confidentiality of a patient's personal medical information. If a patient discloses personal information to a healthcare professional believing it is private, the professional may be liable in tort for disclosure without the patient's consent.[10]

Not surprisingly, medical data often enters the public domain through unplanned and indirect means. For example, signed, consent release forms are obtained by practitioners from patients authorizing them to share personal medical information with others. This type of consent is often used in medicine to allow the transfer of claim information [diagnosis and interventions] for payment by third party payors. As a condition of

care, patients are asked routinely to sign blanket consent forms that authorize disclosure for any lawful use. This type of waiver provides an unrestrained device that can potentially open the door and allow the release of information to others with whom the patient might not anticipate or desire to share such information.

Conclusion

As personal medical information becomes distributed within the environment of electronic record keeping, it takes on an amorphous electronic format that is no longer defined by a sense of place. The sheer magnitude of this data can overwhelm properly installed and well maintained privacy and security restrictions designed to protect personal medical information. In effect, the "private key" has been legally shared with more than one trusted party. All healthcare practitioners and their staff should consider diligence when requesting consent and release forms from patients for sharing medical (or personal) information. These forms allow the wide dissemination of personal medical information in electronic format. The individual's ability to restrict the flow of information and select appropriate recipients is diluted with the conveyance of such consent, or application of waiver.[12]

References

1. Quinn J. Business Building a Web of Personal data on you and me, Seattle Post-Intelligencer, March 9, 2000, p.D1,8.
2. McVeigh v. Cohen, 983 F. Supp 215 (D.D.C. 1998). Description of an ISPs connecting one's identity offline to collected data about their online behavior.
3. Editorial, Privacy on the Internet, New York Times, Feb., 22, 2000, p.A12.
4. Cyberatlas. http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_234841,00.html, accessed 3/11/00.
5. Dyson E. Consumers should control the use of their data on the Net, Seattle Post-Intelligencer, March 11, 2000. B1,4.
6. Norman-Bloodsaw v. Lawrence Berkeley Laboratory 135 F.3d 1260.
7. 42 USC 12112, 5 USC 552 with the 1996 Amendments. Subsec. (a)(2). Pub.L. 104-231, included the option of electronic copying.
8. Spielberg AR. Online without a net: physician-patient communication by electronic mail. Am J Law Med 1999;25: 267-957.
9. Kurtin OD, Noveck BS. National Law Journal, January 24, 2000, p12.
10. Larry Gostin, Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization (1996). http://www.epic.org/privacy/medical/cdc_survey.html
11. Jones v. Prudential Ins. Co. of America, 388 A.2d 476 D.C.,1978.
12. Hicks v. Talbott Recovery System, Inc., 196 F.3d 1226.

(In one consent action, the staff member who designated which records to release did not inform the patient about the sensitive nature of specific disclosures to the state medical licensing board, or explain that the patient could specify non-disclosure of particular treatment records.)

The sanctity of one's personal health records and medical information is a current issue in relation to today's technological abilities and competencies. The question of an individual's confidence in the integrity of their personal medical information and data and the confidentiality of this data is compounded by emotional concerns, ethical mores', and the legal responsibilities of the many parties currently accessing and utilizing this information. On the immediate horizon, congress is designing statutory efforts to provide legislated solutions to these issues.

In a future issue: The next article in this series will discuss these regulatory and legislative initiatives (HIPPA, etc.) crafted to address issues illustrated in this article. How these might affect common information sharing practices and potential liabilities will be examined.

About the Author

James Day, DDS, MEd

Dr. Day is a lecturer in the Division of Information Technology and Research in the Department of Oral Medicine at the University of Washington. He serves as the Vice-Chair of the American Dental Association ANSI Standards Committee for development of electronic technologies and communications in dentistry and a member of the association's Task Force on Distance Learning. Correspondence related to this article can be sent to him at the following address:

Division of Information Technology and Research
Department of Oral Medicine
University of Washington School of Dentistry

e-mail: jimyd@u.washington.edu