the Journal of CONTEMPORARY DENTAL PRACTICE at www.thejcdp.com
Volume 2 Number 1 Winter Issue, 2001

Privacy and Personal Health Data in Cyberspace: The Role and Responsibility of Healthcare Professionals

James Day, DDS, MEd

Abstract

In this series of articles, the author discusses the potential risks, benefits, and liabilities associated with using electronic communications and computer-based records to manage a patient's medical information. This second article in the series considers the role and responsibility of the healthcare professional in collecting and sharing a patient's private personal and medical data in online environments. Current practices and the potential pitfalls of Electronic Data Interchange (EDI) are reviewed.

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

Introduction

Telecommunications and the Internet are part of everyday life and popular culture. Commercialization has distributed the technologies of the computer and cell phone to over 50% of the population. Incredible amounts of information and resources are available online for any specific topic. This includes information that is highly personal and private (e.g., family information). And yet, in spite of this ready access to such personal information, dental professionals continue to routinely store, integrate, and compile personal health data about patients in similar electronic environments with the belief they are secure.

The reality is online security is essentially a misnomer. The recent cyber-infiltration and pilfering of products and source codes from Microsoft's most "secured network" by hackers is evidence that even the foremost developer and provider of software products cannot adequately and totally protect its own data. Of greater significance is a relatively simple and basic hacking tool, "QAZ Trojan," available to anyone on the web was used by the hackers. "The attack proves what many in the Internet security business have said for years: Even the largest corporations and governments are vulnerable to cybercrime."[1]

Everyone has a stake in protecting patient privacy. The challenge is to preserve the integrity of electronic health data. Although no security protocol is 100% effective, a good faith and reasonable approach is needed to achieve the necessary safeguards. This requires an enterprise approach seeking to ensure the integrity and confidentiality of electronically transmitted information.

Time-Honored Model

In the traditional medical model, essential health data is usually gathered and compiled in a direct manner. The primary resource for health information is the medical record. This information is sequentially logged as the patient's health history, examination findings, diagnosis, and treatment that take place over a period of time. The primary source information is garnered through self-report, the compilation of the health provider's findings and recommendations, along with the diagnostic information related through associated tests and referrals. This is considered a "top-down" or "provider-controlled" environment.[2]

Historically this component of information has been and continues to be considered the "patient health record." Generally this record remains available in paper-based format. An electronic form of this information has been distilled into an electronic format for the past 5 to 10 years. This was done in order to facilitate insurance company needs and eventual government requirements for the efficiencies of electronic payment transactions [EDI].[3]

To augment the information provided by the traditional medical record that chronologically documents care as it is provided, a contemporary approach assembles a composite picture of the same information as it is shared electronically. This compilation of information from multiple sources is often associated with either governmental or commercial uses. A question arises as to the effect of such practices of data collection and warehousing in terms of infringement on the rights of the individual and the potential to personally harm an individual through unauthorized disclosure.

Legal Precedence

A court case in New York State reviewed the collection and listing by the state of all patients receiving narcotics through a triplicate state mandated prescription system. The question of whether a data warehouse of computerized patient records actively collected by New York State violated a patient's individual rights to privacy was the subject of a challenge by a group of physicians in 1977.

The state justified the intrusion by offering law enforcement and public health as the justification for the statute. The patient-focused concerns were the risk that medications prescribed might be revealed and possible avoidance of appropriate medical care by the patient because they feared exposure for taking restricted drugs. In this instance, the outcome could easily be less than satisfactory.[4]

In Whalen vs. Roe, The U.S. Supreme Court overturned the New York ruling that collection of personal narcotic prescription data in an electronic database was unconstitutional. The Supreme Court found the privacy of the patient-physician

relationship did not fall within constitutional parameters for privacy. The court added that accumulation of tremendous amounts of personal information in computer data registries indeed threatened the prospect of personal privacy. The court also noted that adequate precautions and protocols preventing disclosure are necessary to protect the public. However, the court found in favor of the state's right to collect personally identifiable health information.[5]

Contemporary Modification

A new and contemporary source for patient medical information is the aggregate of primary health information data that can be compiled from both primary resources and the secondary collection of "related information."

Disaggregated data collected on an individual basis is subjected to a query process. This data is derived from all digital information (from medical to behavioral to financial) associated with the subject in some dynamic manner. A hybrid system for personal healthcare information is generated through two mechanisms:

- Use of technology strategies in new and unique ways (e.g., e-mail)

- Unregulated exchanges of information which occur as a matter of business practice among healthcare providers, insurers, managed care organizations, pharmacies, medical researchers, care benefit managers, social workers, direct marketers of medical products and devices, and others. All of these individuals may have legitimate claim to some portion of an individual's medical record. The magnitude and extent of such a widespread distribution of personal data erodes any systematized practice of privacy and data integrity that one might attempt.[6]

For example, the writing and fulfillment of a pharmacy prescription is considered primary healthcare information and as such is protected as confidential patient-physician communication under most state laws. However the integrity of this information is challenged as it transits the system. After the information is distributed to a pharmacy database, the Electronic Communications Privacy Act allows both proprietary and discretionary use of the received and derived data for internal and business use.[7, 8]

The additional collection of retail credit card and e-commerce data generated through the fulfillment, supply, marketing, and distribution of a medically prescribed product uses alternate communication channels with different protocols, standards, and criteria for security and privilege [ECPA] for shared use.[9] This type of data exchange employs separate security and transaction standards based upon protocols supported by the American National Standards Institute and the Data Interchange Standards Association.

The potential complications and complexities arise when these alternative and collateral channels are used. Multi-agent networks with shared communication capabilities and protocols and softbots with artificial intelligence and natural language functionality can collate this information and profile the user.[10] These agents can select computer files, analyze word occurrence, and summarize the information as keyword components. Other information in selected domains can then be analyzed for matches using the summary to identify and attribute clusters of documents using the same keywords.

These software capabilities effectively collate information allowing the same outcome as if looking directly at the individual's patient record. If the patient has filled prescriptive requests, the commercial information can then be [legally] shared through business relationships with pharmaceutical corporations or direct marketers and promoters representing the drug manufacturers. If the profile is for a disease-specific medication, a profiling of the individual can be accomplished that is as accurate and devastating as a release of primary source information from the physician.[11,12]

The situation is clearly defined in Weld v. CVS Pharmacies. In 1998, Consumer Value Stores (CVS) initiated a Patient Compliance Program. This program allowed CVS to send mailings to certain designated customers reminding them to refill their medication prescriptions, provided them information concerning new drugs, or encouraged the customers to discuss the treatment of potential medical conditions with their doctor. Funding for these mailings was provided by the drug man-

ufacturers [also additional defendants].

"CVS contracted with Elensys, a marketing company, to carry out the mailings for this program. The agreement provided that the marketer, Elensys, would receive customer prescription information directly from CVS. [CVS] agrees to provide to Elensys all pharmacy records and prescription information which Elensys and [CVS] mutually agree are necessary for Elensys to render the Patient Compliance Services."

The agreement also contained strict confidentiality provisions that required Elensys to take extensive measures to protect the confidentiality of the patient information provided by CVS. In its affidavit, CVS states that it never gave Elensys access to its database or prescription records and that Elensys had absolutely no information concerning the bulk of CVS customers who were not included in the program. However CVS does not address how much information about the customers included in the program was actually disclosed to Elensys.

Elensys maintains its involvement in the mailing received by the plaintiff [Kelley] was simply the electronic elimination of duplicative names and correction of address errors. Elensys then sent the final list of names and addresses to W.A. Wilde, a mail fulfillment house which Elensys engaged to stuff envelopes and send out the letters. The defendants assert the mailing procedure was also highly technical and required minimum human involvement [prying]. The Elensys agreement with W.A. Wilde also contained strict confidentiality provisions.

The co-defendant drug manufacturers also asserted they were not given CVS customer information or access to CVS's customer databases. Their only involvement was providing CVS with information about the drugs being promoted and the funding of the mailings."[13]

The primary and initial source of patient-based medical information, the patient medical record (a "top-down" resource) places a primary responsibility on the practitioner for the confidentiality of content that is recognized as a legal responsibility in most states. As exemplified in the Weld v. CVS case, primary health data, once a part of the medical record, quickly becomes hybridized and enters a zone of proximal distribution. The distributed data is related in substance to the original data, but is more amorphous and in the process passes through many more layers of exposure and increased risk for public access.

Both patients and practitioners need to be aware that breaches of data integrity and security can and do occur. The primary responsibility for monitoring, safeguarding, and controlling the patient's personal medical information disclosed under privacy medical may also extend contractually to environments and instances [e.g., Weld v. CVS] where the practitioner does not have direct control or jurisdiction.

In another case, the unauthorized release of personal medical information by the University of Michigan ended up on the web in February of 1999. Thousands of University of Michigan health system patients had personal and medical information released over the Internet without knowing it. Using a business tracking system, patients with recent appointments were included in a database that contained Social Security numbers, employment information, birth dates, and their personal diagnosis. A simple administrative error led to the disclosure of personally identifiable medical information to a relatively limited number of web users. "Patients worried their privacy was hurt from the mistaken release of names and Social Security numbers."[14]

Government Initiative

A bill before the US Senate15 would ensure confidentiality with respect to medical records and healthcare-related information and complicates liability for information within medical records by extension of access to:

- Conducting quality assurance activities or outcomes assessments
- Reviewing the competence or qualifications of healthcare professionals
- Performing accreditation, licensing, or credentialing activities
- Analysis of health plan claims or healthcare records data
- Evaluating health plan and provider performance
- Carrying out utilization review, precertification, or preauthorization of services
- Underwriting or experience rating of

health plans
- Conducting or arranging for auditing services

Currently, utilization review, data warehousing, data modeling, quality assessment, and improvement reviews implemented by third party payors or other interested parties may expose the practitioner to liabilities for record and information integrity through a contractual business relationship.[16]

Corrective action to protect personal private medical information is being promoted by the Administration and the Department of Health and Human Services. Because Congress failed to act, a sunset provision in the Health Insurance Portability and Accountability Act of 1996 [HIPAA] legislation granted HHS authority to impose national standards to protect patient medical records as created by healthcare providers, health plans, and electronic clearinghouses.

These proposed regulations protect identifiable electronic health information while stored and transmitted. Data relating to an individual's health, treatment, or payment for healthcare are protected elements. Although information from which the patient's identity cannot be determined is not included within the regulation's scope, the regulations contractually apply to business partners of covered entities.

The proposed regulations also prohibit a covered entity from releasing individually identifiable health information without written consent informing the patient of the proposed use of their health information. Under the regulations, penalties can be assessed amounting to $25,000 per annum per violation, but a patient may not recover for damages greater than is recoverable on a breach of confidentiality action. Healthcare providers must assess potential risks and vulnerabilities for the individual's health information it possesses and develop, implement, maintain, and document the appropriate security measures.

The regulations require the use and disclosure of individually identifiable health information be limited to only what is necessary; i.e., treatment, payment, or activities required for peripheral supportive protocols. Use and disclosure for any other purpose [except certain governmental purposes e.g., law enforcement] is strictly prohibited without the individual's specific written consent.

One of the most controversial elements of the HHS proposal stems from a congressional, not an HHS, decision that the agency's privacy regulations should not pre-empt "more stringent" state law. HIPAA specifically states that, "unless Congress itself determines otherwise, the states should remain free to protect medical data, so long as that protection is at least as extensive as HHS prescribes." This follows after the Department of Labor's implementation philosophy of OSHA compliance.

The legacy of vast quantities of paper-based medical records could remain federally unregulated providing a loophole for information tangent to the legislation.[17, 18]

Conclusion

Technology has been accused of embodying the threat to privacy. The truth is, technology provides an affordance that can simultaneously improve and damage the status of privacy. If exploitation and profit are the true motive, technology can be extremely efficient in the exploitation of data based resources. However, with the appropriate set of operational goals and a uniform set of standards and protocols, technology can afford greater protection for health information. Technologies allow discrete data sets, de-identified data, and encryption as tools to help protect information. When authorized through policy and supported through sanction, communication, and training, this resource provides us a solution for privacy.

References

1. Cook, J, Pope, C., Richman, D., Hacker Attack a Wake-up Call, Seattle Post- Intelligencer, October 28, 2000.
2. Harris,R. The Need to Know vs. the Right to Know, Privacy of Patient Medical Data in an Information-based Society, 30 Suffolk U. L. Rev., p.1191 (Winter 1997).
3. Health Insurance Portability and Accountability Act, Pub. L. 104-191, 42 USC 1320.
4. Rubinstein, H, A Communitarian Look at the Privacy Stalemate, American Journal of Law and Medicine, Summer-Fall 1999 p 203.
5. Whalen vs. Roe, 429 US 589 (1976).
6. Sheehan, J. Keeping Personal Health Information Private,(accessed 11/21/00) http://www.cisp.org/imp/november_99/11_99sheehan-insight.htm
7. Spielberg, A., Online without a Net, Physician-patient communication by electronic mail, American Journal of Law and Medicine, Summer-Fall 1999, p. 267.
8. 18 U.S.C. 2510-2522 Electronics Communications Privacy Act [ECPA].
9. ASC X12, XML/EDI, (accessed 3/12/2000), http://www.disa.org/
10. Anne Eisenberg, Find Me a File, Cache Me a Cache, NY Times, Feb 10, 2000, D1.
11. Weld v. CVS Pharmacy, Inc., 10 Mass.L.Rptr. 217, 1999 WL 494114.
12. 18 U.S.C. 2510-2522 Electronics Communications Privacy Act [ECPA].
13. Weld v. CVS Pharmacy, Inc., 10 Mass.L.Rptr. 217, 1999 WL 494114.
14. Upton J., Michigan Medical Records Accidentally Posted on Web, Detroit Free Press, February 12, 1999.
15. 1999 CONG US S 578.
16. Spielberg, A., Schwartz P., Privacy and the Economics of Personal Health Care Information, 76 Tex. L. Rev. 1, p. 56-67 (1997).
17. Health Insurance Portability and Accountability Act, Pub. L. 104-191, 42 USC 1320.
18. Perkins, N., What Price Privacy? Legal Times, March 13, 2000.

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 Communication in dentistry and a member of the association's Task Force on Distance Learning. Correspondence related to this article and be sent to him at the following address:

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

e-mail: jimyd@u.washington.edu