PATIENT PRIVACY: ISSUES AND CONSIDERATIONS FOR CUSTOMER RELATIONSHIP MANAGEMENT PROGRAMS

A CPM WHITE PAPER

TABLE OF CONTENTS

SECTION 1:
MEDICAL PRIVACY IN THE INTERNET INFORMATION AGE

Physician-patient confidentiality has been a tenet of health care since the writing of the Hippocratic oath. Patients receive treatment with the expectation that the details, although part of a medical record, will remain private. But medical records are used for research, education, coordination of care and insurance purposes in the interest of better healthcare for the consumer. On the one hand, patients want better health, which requires information sharing—on the other hand, they want their records kept private—therein lies the conflict between confidentiality and need to know.

This concern about access to medical records for legitimate purposes in the consumer's best interest has been heightened by the availability of electronic files, integrated care delivery and health data networks. While this technology is designed to improve health, there is a growing public concern because it allows for easy collection and distribution of sensitive medical records. One-third of Fortune 500 companies are believed to check medical records before hiring new employees. And, studies show that patients are lying about their medical histories, paying for care out-of-pocket and going to multiple providers to avoid the creation of a consolidated medical record.

INCONSISTENT STATE GUIDELINES AND A MOVE TOWARD FEDERAL LEGISLATION:

Complicating this issue is the fact that there are inconsistent state policies and no federal guidelines regarding medical privacy. Despite years of effort to standardize these regulations, Congress has failed to pass legislation concerning privacy of medical records because of sharp disagreement over the details and the ramifications of using the information for research and wellness programs—programs designed to have a positive impact on the health of the U.S. population.

It's a complicated issue, particularly because it involves bioethical questions. Therefore, privacy advocates and consumer groups are looking for a tough law that would prohibit health insurance companies, researchers and law enforcers to use records for anything other than care and billing.

The Health Insurance Portability and Accountability Act of 1996 required the Secretary of Health and Human Services to produce health privacy regulations since Congress missed its own August 21, 1999 deadline.

Because Congress did not act, the HHS Secretary's deadline was triggered, and she has an initial target date of February 2000 to provide final health privacy regulations. The date of the release of those regulations may be extended. When released, this set of guidelines won't take effect until TWO YEARS AFTER their adoption. It is predicted these stipulations may allow patients to:

- control conditions under which their medical data could be shared
- learn who else had seen the information
- examine their records and make corrections.

The Secretary is expected to base a significant portion of the draft regulations on her recommendations that were submitted to Congress in 1997. The draft was published in the Federal Register as a Notice of Proposed Rule Making to allow for general comments by the public for 60 days. However, the initial proposal was more than 600 pages, revealing not only the complexity of the issue but also the difficulty in getting consensus on a document that ultimately may be too general to have any staying power.

Nonetheless, President Clinton says the plan, dubbed a "Patients' Bill of Rights," is "an unprecedented step toward putting Americans back in control of their own medical records." He has recommended that improper use of records by a healthcare organization or insurer could result in civil and criminal penalties.

FINDING A BALANCE:

Where is the balance for patients in this process? How do you ensure advances in treatment through information sharing and physician collaboration while respecting privacy? When does one good outweigh the other?

Technology has made the issue more thorny than ever. Development of customer profiles in massive databases accessible with data mining techniques, provides organizations with knowledge to better serve individuals' preferences and needs. And the Internet makes it easy to send these databases virtually anywhere. Yet, consumers don't want to lose trust in their favorite businesses and providers if they feel personal information has been shared or used for other purposes without their consent. It seems there are more questions than answers.

How can organizations walk the fine line between providing welcome customer value and unwelcome intrusion on patient privacy? What can and should healthcare organizations do to mitigate consumer concerns in their Customer Relationship Management (CRM) programs on the basis of these worries and pending legislation?

SECTION 2:

ADDRESSING CURRENT AND PENDING PATIENT CONFIDENTIALITY LAWS: WHAT YOU CAN DO

One way to respond to the friction between serving patients' individual interests and confidentiality versus advances in healthcare for the public good, is to add data privacy policies to your CRM initiatives. This strategy can help you avoid legal ramifications and loss of patient loyalty. It must be based on an understanding of current and proposed patient privacy regulations and take into consideration:

- Federal laws are under discussion and could be finalized **at any time**.
- There is a two-year compliance period following final acceptance—ensuring the laws will not go into effect until **at least** February 2002.
- The proposed regulation language is ambiguous, with some words loosely defined and arguable, including key terms such as "disclosure."

TERMS AND DEFINITIONS:

For all uses and disclosures of health information, healthcare organizations should obscure personal identifiers as much as possible, while maintaining the usefulness of the data. Based on one interpretation of the laws, identifiable medical information cannot be used for marketing communications without patient consent. This paper assumes that interpretation is correct.

But using data for the case management of illness and diseases is permissible. It is debatable whether community and individual awareness, wellness, and educational communications constitute marketing or in some cases, outpatient management, which is a permissible use.

Healthcare organizations need to consider the following terms and definitions as they look at their consumer databases and communication programs:

- "Medical Information" includes DRG, ICD-9, MDC and CPT-4. These do not include demographics.
- "Patient Identifiability" includes name, address, social security number, medical record number, telephone number, or any other unique identifier.
- "Marketing Communications" includes healthcare communications and can be grouped into four categories:

  a) Awareness—Creating an awareness of your organization in your market area

  b) Wellness—Creating an awareness of public wellness through screenings, classes, health fairs, etc.

  c) Intervention—Communications that assist in the outpatient management of an illness.

  d) Chronic Disease—Communications that assist in the outpatient management of a chronic disease or illness.

STRATEGIES:

Keeping current regulations in mind and assuming full adoption of proposed regulations, the following steps can help you mitigate your risk:

1. Immediately institute procedures to gain patient consent at all contact points for relevant healthcare communications. During their first encounter with the organization, all patients should have the opportunity to consent to inclusion in your communications programs. Adding a brief paragraph to current treatment consent forms and an opt-out selection on your Web site should not pose any major operational problems.

2. Sign a Business Partner Agreement. A business partner is an organization that acts as an extension of your organization and assumes all rights and responsibilities of the healthcare organization. The current proposed regulations have defined points in a formal Business Partner Agreement, that more than likely are already covered in existing contracts. The Business Partner Agreement is simply a formally defined procedure.

   The agreement will give your provider access to medical data for the purpose of database construction and analysis, while using the identifiable medical data for communications is a different issue. Both hospitals and business partners have an ethical responsibility to maintain public trust by keeping healthcare information confidential. They are accountable for the ways they use, maintain and disclose personally identified information. Any agreement should safeguard or protect unauthorized use or disclosure of the data. Healthcare providers and business partners should agree to adhere to the standards as they are finally adopted.

3. The data you use to construct your database should not include chemical dependency, HIV or psychological encounters or information. This is very sensitive and personal information and its use may increase your overall exposure to risk.

4. Build your database so it obscures any individually identifiable information (as defined above) during list selection and analysis. Selections are generally viewed in the aggregate, not individually; therefore not having patient-identifiable information doesn't hamper the database's analytical use. The selection program can generate a set of "links" to the selected names and addresses, which can be used by a separate application that can only "see" the names without any medical information. This eliminates simultaneous viewing of the medical data and the identifier.

   Patient consent is not necessary for the use or disclosure of non-identifiable health information. When health information doesn't link to individually identifiable information, privacy concerns are greatly reduced. For example, many diseases are tied to gender and age. Marketing programs to women over age 30 about breast cancer risk or to men over 40 about colon cancer screening can be implemented without the use of personally identifiable information.

5. Add a market area list, which contains all the individuals living in your service area, to your database. The market list is a super set containing all individuals in your market area, but lacks the depth of information contained in your operational systems. Having this data merged into your database allows you to state the source of the information used in the list selection was the market list, not information collected internally. The added value of this market list is new names and addresses of those who are not currently patients.

6. Add market/consumer segmentation information, such as CPM's Consumer Healthcare Utilization Index™, (CHUI) to your database and use this as selection criteria. CHUI™ is a predictive tool that provides a score from 0-999 that indicates an individual's propensity to need services as defined by the major diagnostic categories (MDC). All targeted list selections can be based on geography and demography from the market list, plus the CHUI™, none of which include protected patient information.

7. Limit use of medical information to:
   - Selection exclusions. For example, exclude individuals already identified with diabetes from a communication about a diabetes screening program
   - Outpatient case management. Sending information that will help individuals better manage specific illnesses and diseases is permissible to improve patient wellness. For example, you might do a mailing about cardiology tests to individuals who have had cardiology-related outpatient visits. As indicated earlier, use of information for case management is allowed under the proposed guidelines.

8. Design all communication packages consciously with an "opt-out" mechanism. This includes all communication channels—direct mail, inbound calling, and electronic. Preference should also be indicated by communication channel. An individual should have the option to say direct mail messages are okay but not e-mail. Once an individual has opted-out, immediately mark the name as "do not contact." You should also immediately flag any deceased individual as "deceased" and remove them from any communications program. Make sure your systems are rapidly updateable.

SECTION 3:

CONCLUSION

In the last 20 years of healthcare marketing, CPM has never experienced any consumer complaints regarding invasion of privacy or misuse of medical information. We believe this indicates that properly designed communication programs can be executed responsibly while fulfilling the needs of the patients and community at large.

In addition, the knowledge embodied in your data may be the most powerful resource for the ongoing management of customer relationships and your organization's development in today's highly competitive world.

Put your information to work, but be aware of how to use it responsibly.

SECTION 4:

ABOUT CPM

Customer Potential Management (CPM) Corporation is an international leader in solving social and business problems through integrated customer information marketing databases.

CPM's Customer Relationship Management (CRM) solution allows healthcare providers to manage their customer relationships through targeted, personalized communications, which build loyal long-term patient relationships. Designed and maintained by CPM, this Internet-based information database provides individual customer information to answer who, what, where, when and why questions about past, current and prospective patients. Our intelligent CRM pieces fit together seamlessly into an application framework that produces a single, top-level business strategy.

For more information, contact us:

Customer Potential Management Corporation
Business and Marketing Intelligence for the Healthcare Industry
2500 N. Main Street, Suite 2
East Peoria, IL 61611
800-332-2631/309-698-1037
FAX 309-698-1039
www.cpm.com
Email: sales@cpm.com