

# Marketing to Patients: A Legal and Ethical Perspective

Deborah M. Gray PhD  
Central Michigan University  
mosca2dm@cmich.edu

Linda Christiansen, JD MBA  
Indiana University Southeast  
lchristi@ius.edu

## ABSTRACT

Medical practices and other healthcare providers are frequently reluctant to use medical records in marketing as a result of misconceptions regarding HIPAA law. Healthcare providers should have no qualms about using medical records or offering a service such as email for communication with patients for fear of violating HIPAA. Their concerns should lie only within the concerns for ethical online marketing, albeit with a greater sensitivity for how patients might react to usage of what is considered by many to be very private information.

Keywords: Marketing, Ethics, HIPAA, Healthcare, Professional Codes of Ethics

## Introduction

The healthcare industry appears to be avoiding use of email and Web marketing as a result of concerns regarding HIPAA restrictions and warnings from insurers not to engage in electronic communication with consumers (Landro, 2002). In this paper we address the use of electronic marketing strategies (email marketing, online scheduling, etc.) in the healthcare field within the confines of the HIPPA law and industry-recommended ethical guidelines. Offering these customer-oriented services can be a strategic use of the Internet for marketing to current patients, attracting new patients, and reducing costs. Web and email marketing are ripe marketing options for medical practices because consumers are increasingly using the Internet as a means of searching for information about their health concerns (HarrisInteractive, 2007). Today's patients are very interested in being able to contact their physician by email to schedule appointments and/or ask questions (HarrisInteractive, 2007). However, these services must be offered within the realm of legal rules (HIPPA) and ethical guidelines set forth by industry codes of ethics.

Research clearly shows that Americans are avid users of the Internet for healthcare matters. According to industry reports from 2004, 78% of American consumers have Internet access and 97% have email access at home, work, or via a friend (HarrisInteractive, 2004). In that study, nearly 74% of U.S. adults reported that they use the Internet to search for medical information (HarrisInteractive, 2004); and in 2007, another 58% felt so empowered by the available information that they brought those concerns to their physician (HarrisInteractive, 2007). The number of people who have searched for medical information online has seen a 37% increase in the two year period from 2005 to 2007 (160 million in 2007 from 117 million in 2005) (HarrisInteractive, 2007). HarrisInteractive has coined the term 'cyberchondriacs' to describe the 84% of adults who go online to search for medical information (HarrisInteractive, 2007). As long ago as 2000, 54% of consumers felt strongly enough about email communications to schedule appointments, renew prescriptions, or check lab results that they would be willing to switch doctors to one who offers such (Coile, 2000). Taken together, most people are searching for health-related information online, and they are discussing that information with their doctors. More than half want to use email in some capacity to communicate with their doctor. What does this mean to doctors, healthcare professionals and medical practices?

"The huge and growing numbers of "cyberchondriacs" who use the Internet to look for health information and to help them have better conversations with their doctors has surely had a big impact on the knowledge of patients, the questions they ask their doctors and is therefore changing the doctor-patient relationship and the practice of medicine. There is every reason to believe the impact of the Internet on medical practice will continue to grow." (HarrisInteractive, 2007)

It is clear that if medical practices are going to reach consumers with information about their services or engage in customer retention activities, they cannot ignore email and Web marketing strategies. However, they also cannot ignore the law or ethical standards set forth by the marketing industry. The constraint then for taking advantage

of online marketing strategies in the medical field is two-pronged – both legal and ethical. From a legal perspective, many people have the misconception that HIPAA prohibits any release or use of medical information for most reasons. Bizarre interpretations of the law range from the cancellation of birthday parties for nursing home residents for fear of revealing a resident's date of birth to assigning nonsense code names in lieu of patient names for summoning people from doctor's waiting rooms. Some medical personnel have taken to blaming HIPAA when refusing to reveal medical information, whether by innocence or intentionally (Gross, 2007). Once healthcare organizations overcome the 'fear' of HIPAA, they must then take into consideration the ethical guidelines from organizations like The American Marketing Association and The Direct Marketing Association.

This paper addresses the legal and ethical concerns for marketing methods which use the Internet or other forms of electronic media to market to current patients using their medical records.

### **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

HIPAA was enacted in 1996 because, among other reasons, Congress wanted to reduce the cost of administrative operations in the healthcare industry. Electronic transfer of healthcare information was becoming more prominent and was thought to be part of the solution. The act sought to simplify the exchange of electronic information, while also guarding against fraud and unauthorized access and disclosure to health information. As with many substantial passages of laws, Congress delegated the duty to issue regulations to a federal agency, the Department of Health and Human Services (HHS), regarding the how, when, and to what extent private health information can be disclosed (HIPAA sections 261-264).

The major goal of the Privacy Rule is to protect patients' health information while striking a balance to allow for sufficient flow of medical information to provide high quality health care and to protect the public's health and well-being (Office of Civil Rights, Summary of the HIPAA Privacy Rule 4).

The Privacy Rule covers all "protected health information" (PHI), which includes all individually identifiable health information that is held or transmitted by the covered entity or its business associate.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and

- (1) Is created or received by a health care provider, health plan, employer, or healthcare clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - (i) That identifies the individual; or
  - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual (45 CFR 160.103).

For purposes of HIPAA, "covered entities" include (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. A

"healthcare provider" is defined as "a provider of services, a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business" (45 CFR 160.103, 104).

### **Misconceptions Corrected: HIPAA Does Not Restrict Marketing by Doctors to Current Patients**

For purposes of HIPAA, "marketing" is defined as "a communication about a product or service, a purpose of which is to encourage recipients of the communication to purchase or use the product or service, subject to certain limited exceptions." Under this general rule, a healthcare provider must obtain a patient's authorization to use or disclose protected health information for marketing communications (45 CFR 164.501(1)).

HIPAA rules, however, provide for exceptions to this general marketing rule. One such permissible exception occurs when a covered entity uses a patient's protected health information. The U.S. Department of Health & Human Services (HHS) states specifically on its website that "the HIPAA Privacy Rule excludes from the definition of "marketing" communications made to describe a covered entity's health-related product or services ...that is provided by, or included in a plan of benefits of, the covered entity making the communication" (Health Information Privacy and Civil Rights Questions & Answers, Question 281):

The HHS website includes an example in which a physician who has developed a new anti-snore device sends a flyer to all of her patients - regardless of whether they had previously sought treatment for that ailment. This plan is specifically presented as allowable marketing under HIPAA. The hypothetical example clearly shows that physicians and medical practices can offer information regarding its own products or services to any current patient.

### **Consulting by Business Associates**

If a doctor wishes to market to current patients, he or she has the option of hiring a marketing consultant or firm to aid in this endeavor. HIPAA allows for this type of outsourcing to outside experts under the definition of "business associates."

A business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in Sec. 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person (45 CFR 160.103).

## **HIPAA Intent and Penalties**

Just to clarify, this exception to the HIPAA marketing restrictions regarding the use of a marketing consultant applies only to the physician's or covered entity's use of advertising products or services to current patients, not the advertising for a third party, nor the sale of protected health information to a third party for the marketing use to benefit that third party.

Understandably, some medical practices are reluctant to market to current patients for fear of violating HIPAA. Penalties for violating HIPAA can be substantial, amounting to a maximum fine of \$250,000 and 10 years in prison for certain cases (42 USC 1320d-6(a)(3)). However, physicians have so much to gain through educated understanding of allowable uses of electronic marketing.

Ironically, physician marketing to existing patients was not the intent of Congress when it developed the HIPAA restrictions, yet according to the letter of the law, a doctor could technically be caught in its web. The intent of the Act is to protect patients from unauthorized access to personal health information when it is transmitted electronically to third parties, such as insurance companies or testing facilities. Yet when doctors use electronic means to market additional services to current patients, they must be very careful as to limit the personal information transmitted so as to avoid any HIPAA issues.

## **HIPAA Covers Electronic Transfers Only**

45 C.F.R. 164.104 states that the regulations apply to "covered entities" which include "(3) a healthcare provider who transmit any health information in electronic form in connection with a transaction covered by this subchapter" (45 CFR Subtitle A Part 164.104(1)(3)). Note therefore, that HIPAA regulations do not cover non-electronic forms of transmission of health information. In other words, HIPAA regulations do not in any way restrict the usage of personal medical records for marketing purposes if those contacts are made by non-electronic means.

## **The HIPAA Privacy Rule**

If HIPAA applies, what are the requirements? Section 164.306(a) requires that "covered entities" must:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains,

or transmits; (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; (4) Ensure compliance with this subpart by its workforce.

Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. The regulations allow for structure of the organization and a cost-benefit analysis to be considerations in determining security measures.

### **Additional Jurisdictional Considerations**

Thus far, our discussion has been limited to HIPAA, which is a federal statute. Each state has the option to regulation the usage of patient information as well. Generally, the HIPAA Privacy Rule preempts all conflicting state laws, unless the state law is stricter, with some exceptions relating to public policy issues (Summary of the HIPAA Privacy Rule 4, 2003). Admittedly, it can be quite difficult to discern whether the state law is more stringent or contrary to the federal regulations, so state law should also be considered (State Health Privacy Laws, 2002) in the development of a marketing plan.

### **Marketing Ethics**

Medical professionals need to study and reflect beyond the legal restrictions imposed by HIPAA. In regards to marketing, medical professionals should employ a three-tiered approach in evaluating the appropriateness of behavior. First, the intent of law is generally thought to be the minimum acceptable behavior, rather than the ideal. Second, ethical standards demand more in that they are based on what is right, rather than the minimum that will be enforced by the legal system. Finally, marketing activities by definition carry the even greater burden of attracting and appealing to the target audience.

Though the American Medical Association has an extensive code of ethics, it does not specifically address the issue of marketing to patients—the focus is on dedication to the best interest of the patient’s health which includes following the law (American Medical Association, 2008). Of course this is no surprise since the American Medical Association is a medical association. The American Marketing Association (AMA) serves all organizations who engage in any form of marketing, including Internet marketing. The Direct Marketing Association (DMA) serves organizations that market directly to the consumer; therefore the DMA has more specific and rigorous ethical guidelines for online marketing. The AMA Code of Ethics requires that members conform to three ethical norms of conduct and 6 ethical values (AMA Code of Ethics, 2008).

- “Marketers must do no harm.”
- “Marketers must foster truth and trust in the marketing system.”

- “Marketers must embrace, communicate and practice the fundamental ethical values that will improve consumer confidence in the integrity of the marketing exchange system. These basic values are intentionally aspirational and include honesty, responsibility, fairness, respect, openness and citizenship.”

Within its Code of Ethics, the AMA defers to sub-disciplines to create and define industry-specific codes of ethics.

The DMA is one of these industry sub-disciplines. The DMA has 54 articles within its 31-page “Guidelines for Ethical Business Practice, including articles 38-43 which address online marketing (DMA's Guidelines for Ethical Business Practice, 2008). Table 1 summarizes the contents of articles 38-43. The DMA ethical guidelines focus primarily on providing notice and consent to consumers. Note however, that the DMA does not discourage marketers from using cookies (small pieces of software placed on your computer that identify you—without cookies your login information is not saved on a Web site, for example). Marketers who follow The DMA guidelines will mention the use of cookies somewhere in their privacy or terms of use statement. We also note that the DMA does not actively encourage ‘permission-based’ marketing within their ethical guidelines (nor do they discourage it).

Table 1  
Summary of The DMA Guidelines for Ethical Business Practice

Article	Summary of Ethical Guidelines
38: Online Marketing	Marketers must provide notice, honor choice, provide access, provide data security, abide by laws and ethical guidelines that apply to marketing to children under the age of 13, and demonstrate accountability.
39: Commercial Solicitations Online	Marketers may send commercial email solicitations if they are sent to the marketers own customers, or the customer has agreed to receive solicitations, or the customer did not ‘opt out’ when given the choice to do so. Within each email solicitation marketers must provide customers with a notice and an Internet-based way to refuse future solicitations or request that the marketer not rent, sell, or exchange their email information for online solicitation purposes.
40: E-Mail Authentication	Marketers that use email for communication and transaction purposes should adopt and use protocols that readily identify who they are.
41: Use of Software...	Marketers should not deceptively install or use software that interferes with the consumers computer including software that produces endless loop pop ups, viruses, or spam. If the marketer does install software on the consumer’s computer the marketer must provide notice and a method for uninstalling the software. This article does not govern the use of cookies. Cookies are governed

	by article 38.
42: Online Referral Marketing	Online referral marketing includes encouraging the consumer to forward information to another consumer <i>or</i> to provide the marketer with personally identifiable information about another person (e.g. a friend's email address). The guidelines in this article only apply to the second item aforementioned and require that if the marketer is going to engage in using email addresses provided by another consumer, the marketer must tell the referring user what the information will be used for. They must also disclose if the referring users own information will also be used and disclose to the referred individual that their information was obtained by a referral, and provide a way for all individuals to be removed from future contact.
43: E-Mail Appending to Consumer Records	Email appending is the act of connecting an individuals' email address to another record (e.g. name, physical address, etc) via a third party database. Marketers should append consumer records only when the consumer gives permission to do so, <i>or</i> when there is an established relationship with the consumer, <i>or</i> the consumer did not 'opt out' via the third party database collector, and efforts are made to verify the accuracy of the append. All messages to an e-mail appended address should disclose notice and choice to continue to communicate via email.

## Marketing Considerations in Healthcare Industries

However, if healthcare organizations choose to offer these services, they should also follow the DMA Ethical Guidelines requiring that all emails include a notice and an Internet-based method for 'opting out' of future email solicitations. Because of the sensitivity of health-related information we believe healthcare organizations should take *extra* precaution when using online strategies by using only an 'opt in' approach, otherwise known as permission-based marketing. While it is within the DMA guidelines to contact consumers until or if they 'opt out', consumers are understandably sensitive when it comes to their healthcare-related information. It is therefore not only ethical, *but judicious*, to adopt an 'opt in' strategy for medically-related online marketing strategies.

The medical industry has missed an opportunity to market to patients and to offer patients value by offering services via email because of fear of violating HIPPA regulations. This need not be the case. From a legal and ethical perspective, as long as medical practices do not sell or rent a patient's personal information to a third party, they can use email to market to new and existing services to patients without breaking the law or ethical guidelines set forth by the DMA. Moreover, they can offer value-added services which will likely result in gaining new patients. The three tiered approach is not only legal and ethical, but judicious: follow the HIPPA Law, operate within the guidelines



of industry ethical standards, and carry a greater burden of asking “Will I offend my patient/customer,” “What concerns might my patient/customer have with this strategy?”

## References

42 USC 1320d-6(a)(3), (HIPAA Sec. 1177)

45 CFR 160.103 (2002).

45 CFR 160.103, 104 (2003).

45 CFR 164.501(1), Federal Register, Vol. 67, No. 157, August 14, 2002, pp. 53183-4, <http://www.hhs.gov/ocr/hipaa/privrulepd.pdf> (last accessed August 23, 2008).

45 CFR Subtitle A, Part 164.104(a)(3), [http://www.access.gpo.gov/nara/cfr/waisidx\\_06/45cfr164\\_06.html](http://www.access.gpo.gov/nara/cfr/waisidx_06/45cfr164_06.html), (last accessed August 23, 2008).

American Marketing Association Statement of Ethics (2008), <http://www.marketingpower.com/AboutAMA/Pages/Statement%20of%20Ethics.aspx>, (last accessed August 23, 2008).

American Medical Association Principles of Ethics (2008). <http://www.ama-assn.org/ama/pub/category/2512.html> (last accessed August 23, 2008).

Coile, Russell C. Jr (2000). E-health: Reinventing healthcare in the information age. *Journal of Healthcare Management*, 45(3), 206-10.

Direct Marketing Association's Guidelines for Ethical Business Practice (2008) <http://www.dmaresponsibility.org/Guidelines/>, (last accessed August 23, 2008)

Gross, Jane, "Keeping Patients' Details Private, Even From Kin," The New York Times, July 3, 2007, [http://www.nytimes.com/2007/07/03/health/policy/03hipaa.html?\\_r=1&oref=slogin](http://www.nytimes.com/2007/07/03/health/policy/03hipaa.html?_r=1&oref=slogin) (last accessed August 23, 2008).

HarrisInteractive (2007). “Harris Poll Shows Number of “Cyberchondriacs” – Adults Who Have Ever Gone Online for Health Information– Increases to an Estimated 160 Million Nationwide, *The Harris Poll #76*, July 31.

HarrisInteractive (2004). “No Significant Change in the Number of ‘Cyberchondriacs’- Those Who go Online for Medical Information, [http://www.harrisi.org/news/newsletters/healthnews/HI\\_HealthCareNews2004Vol4\\_Iss007.pdf](http://www.harrisi.org/news/newsletters/healthnews/HI_HealthCareNews2004Vol4_Iss007.pdf), (last accessed January 24, 2007), 4 (7).

Health Information Privacy and Civil Rights Questions & Answers, Question 281,  
<http://www.hhs.gov/hipaafaq/use/281.html> (last accessed August 23, 2008).

<sup>1</sup> 45 CFR 160.103 (2003).

HIPAA sections 261-264, <http://aspe.hhs.gov/admsimp/pl104191.htm> (last accessed August 23, 2008).

Landro, Laura (2002) "New Guidelines to Make Doctor-Patient E-Mails Profitable, Less Risky" *Wall Street Journal (Eastern Edition)*, New York, N.Y.: Jan 25 pg A. 13.

Office for Civil Rights, U.S. Dept. of Health & Human Services, Summary of the HIPAA Privacy Rule 4 , p. 1, last revised 05/2003,  
<http://www.hhs.gov/ocr/privacysummary.pdf>, (last accessed August 23, 2008).

State Health Privacy Laws (2nd edition, 2002), [www.healthprivacy.org](http://www.healthprivacy.org) at  
[http://www.healthprivacy.org/info-url\\_nocat2304/info-url\\_nocat.htm](http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm), (last accessed August 23, 2008).

