Legal Department – New York Office
224 West 30th Street, New York NY 10001
Tel: 212.760.3100 Fax: 212.760.3222
www.medscape.com cbs.healthwatch.com

PRESENTATION ABSTRACT

DATE: MARCH 2ND, 20001

TOPIC: SELF-REGULATION OF HEALTH CARE WEB SITES AND HIPAA ISSUES

SPEAKER: MARK E. BOULDING, GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT, GOVERNMENT AND REGULATORY AFFAIRS, MEDSCAPE

PROGRAM: CONCURRENT SESSION 607: "INDUSTRY SECTOR HIPAA COMPLIANCE: E-HEALTH COMPANIES AND ETHICS," GIVEN AT THE SECOND NATIONAL HIPAA SUMMIT, WASHINGTON, DC.

OVERVIEW

My presentation will cover the interaction of the Hi-Ethics self-regulatory code for health web sites with HIPAA, as well as some general web site privacy issues. I will also discuss special problems and sensitivities that web sites in the health care area face.

HI-ETHICS CODE

The explosive growth of the Internet and the World-Wide Web has given health care professionals and consumers access to almost limitless amounts of medical and scientific information. Some of this information is provided by the government, some is provided by individuals or charitable/academic organizations, and some is provided by commercial entities. In addition, many observers predict that some or all of traditional medical care will move online in the next few years (the online pharmacies are leading the way). In response to concerns about ethical issues and privacy of sensitive information, various self-regulatory initiatives have emerged (listed in order of first appearance of a draft):

1. The Health on the Net Foundation Code ("HonCODE"), a short and straightforward code that is largely self-policing (www.hon.ch).
2. The eHealth Ethics Code, sponsored by the Internet Healthcare Coalition (www.ihealthcoalition.org).
3. The Hi-Ethics Ethical Principles, a product of a coalition of largely commercial health web sites (www.hiethics.org)
4. The AMA Guidelines for Medical and Health Information Sites on the Internet, which come from the American Medical Association (www.ama-assn.org)

Other presentations address the HonCODE, the eHealth Code, and the AMA code. In this document, I will briefly cover the history and content of the Hi-Ethics Code.

Hi-Ethics, or Health Internet Ethics, was formed in November 1999 to address privacy, advertising and content quality issues for Internet health consumers. Member companies donated the skills and knowledge of their executive leadership to develop the principles. Because the Hi-Ethics organizations represented a significant portion of the Internet health space, they were able to make a swift and direct positive impact on the consumer's Internet health experience. According to the Media Metrix report in March, all Hi-Ethics sites listed with Media Metrix, combined, had 11.5 million unduplicated unique users or 15.9% reach of all Internet visitors.

The Hi-Ethics principles state that Hi-Ethics companies will provide online health services that reflect high quality and ethical standards, and to that end they are dedicated to meeting the goals of:

- Providing health information that is trustworthy and up-to-date;
- Clearly identifying online advertising and disclosing sponsorships or other financial relationships that significantly affect content or services;
- Keeping personal information private and secure, and employing special precautions for any personal health information; and
- Empowering consumers to distinguish online health services that follow the principles from those that do not.

The Hi-Ethics Code contains principles in the following detailed areas:

- General privacy policy: fair information practices
- Enhanced Privacy Protection for Health-Related Personal Information

- Safeguarding Consumer Privacy in Relationships with Third Parties
- Disclosure of Ownership and Financial Sponsorship
- Identifying Advertising and Health Information Content Sponsored by Third Parties
- Promotional Offers, Rebates, and Free Items or Services
- Quality of Health Information Content
- Authorship and Accountability
- Disclosure of Source and Validation for Self-Assessment Tools
- Professionalism
- Qualifications
- Transparency of Interactions, Candor and Trustworthiness
- Disclosure of Limitations
- Mechanism for Consumer Feedback

In the press release announcing the principles, Hi-Ethics members committed to becoming compliant with them by November 1, 2000. Current Hi-Ethics member companies include adam.com, allHealth.com/iVillage, America Online, AmericasDoctor, CareInsite, Discoveryhealth.com, drkoop.com, HealthCentral.com, Healtheon/WebMD, HealthGate, HEALTHvision, Healthwise, InteliHealth, LaurusHealth.com, Mediconsult/Physicians'Online, MedicaLogic/Medscape, OnHealth, PersonalMD, PlanetRx, and WellMed

PRIVACY ISSUES FOR HEALTH WEB SITES

A significant area of concern for any developer of a web site is the privacy of information collected from users. The convention on the web (not as widely followed as some would like) is to implement a privacy policy that lets people know how their information will be user. In the health care area, there are special concerns about the sensitivity of treatment information and disease state that may require the development of a more advanced form of privacy policy.

General Privacy Policy Issues

A traditional privacy policy should address the following areas (known collectively as "fair information practices"):

1. **Notice:** users should be given enough information about how their personal information will be used to make a decision concerning whether they want to use a particular web site.
2. **Choice:** Users should have a meaningful choice about how their information is used (including the choice not to use a web site at all, and to avoid collection of any data about themselves).
3. **Access:** Users should have access to information and tools that help them understand and control how their information is used.
4. **Security:** User information should be subject to appropriate protections.
5. **Contact information:** Web sites should provide an effective means of contact for users to report privacy concerns or ask questions about use of their information.

Occasionally, "Enforcement" is mentioned as an additional component, although most web site privacy policies only address enforcement by reference to third parties (for example, TRUSTe). Once a privacy policy is in place, it binds the owner of the web site to its terms. Failure to follow the policy may result in FTC or state action.

A number of online resources that can help in the creation of privacy policies exist, including one web site (from the OECD) that will actually generate a policy in response to a series of detailed questions about proposed uses of information (http://www.oecd.org/scripts/PW/PWHome.ASP). Some good general resources on web site privacy are available on the EPIC web site (www.epic.org). In addition, a special law was recently passed to protect the privacy of children online. More information is available in the attached materials or on the FTC's web site (www.ftc.gov).

Special Privacy Issues for Health Web Sites

Public scrutiny of the way health care web treat health-related information they gather from their users is increasing. Recently, the California Healthcare Foundation (http://www.chcf.org/) released the results of two projects on health care web sites:

1. A survey that found consumers distrustful of web sites when it came to sharing their personal health information.
2. A report that raised issues as to whether many health care web sites were following their own privacy policies.

The Foundation report also focused on activities of ad serving companies and identified a serious potential leak of confidential information from health care web sites to these companies. The report received national press coverage, and some of companies involved (both health care web sites and ad serving companies) are under investigation by the Federal Trade Commission.

Recently, two groups (the Internet Healthcare Coalition and Hi-Ethics) have drafted proposed codes of ethics that address the special requirements of healthcare web site privacy policies. Some suggestions for additional points for privacy policies that have come out of these and other efforts include:

1. Applying an "informed consent" model to notice to users (so that individuals receive specific notice of the type of proposed use and limitations, as opposed to a blanket statement).
2. Allowing users to amend their information or limit use of particular aspects of it on an individual basis.
3. Creating internal systems, including policies and procedures for employees, physical security systems, and audit trails, to ensure that confidential healthcare information is protected.

Many of these points are similar to requirements that will become law for health care plans, providers, and healthcare information clearinghouses under the final HIPAA regulations on health

information privacy. In addition, the final HIPAA privacy regulations, includes features like:

1. Expiration dates for consent
2. Specific forms of notice
3. Limitations on uses by partners
4. Acknowledgment of financial gain from disclosure
5. Special rules for research uses, including creation of a "privacy board" with independent members to oversee research.

The effective date of the HIPAA regulations is almost two years away, and there are efforts to persuade the new administration to alter or even revoke the regulation. In addition, it seems likely that Congress will enact privacy legislation for web sites in the next session. However, despite these uncertainties, and despite the fact that HIPAA probably does not even apply to many consumer healthcare information web sites, some web sites are considering incorporating portions of the final regulation into their privacy policies (to assure "best practices").

AUTHOR INFORMATION

I am the General Counsel and Executive Vice President, Government and Regulatory Affairs of Medscape, a provider of software and services to health care professionals and online health care information. Our products include a web site for healthcare professionals, medscape.com, and one for healthcare consumers, CBS.Healthwatch.com, as well as the electronic medical records application "Logician." Prior to joining Medscape, I was an attorney in private practice, where I specialized in health care and technology law, with a particular focus Internet-based companies, government regulation, and healthcare e-commerce.

You can reach me in the following ways:

1. By phone: 212-760-3271 or fax: 212-760-3222
2. By email: mboulding@medscapeinc.com
3. On my web site: www.boulding.com

20500 NW Evergreen Parkway
Hillsboro, OR 97124
www.medscape.com
www.cbshealthwatch.com

HIPAA 2001 for Medscape Customers

Introduction

This document will outline the final privacy and transaction rules for the Health Insurance Portability and Accountability Act (HIPAA.) This document will discuss these new Federal regulations and their impact on Medscape customers. This document is meant to serve as an aid for customers to use in becoming HIPAA compliant. As of the date of publication of this white paper, there are other HIPAA regulations that have not yet been finalized, and this paper does not discuss them.

Table of Contents

Information contained within this document should not be construed to be legal advice. This document is informational only. You should contact your attorney for advice should you need it.

Overview

Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) on August 21, 1996. HIPAA was enacted because Congress recognized the need for efficiencies and cost savings within the health care industry that electronic technology could provide. They wanted to require standards for electronic information, and they wanted to provide privacy protections for electronically transmitted health information. Because Congress failed to enact the HIPAA legislation by the August 21, 1999 due date the department of Health and Human Services (HHS) developed and published their proposed HIPAA regulations. The HHS HIPAA regulations are in the areas of Privacy, Security, Transactions and Code Sets, National Provider Identifier (NPI), and National Employer Identifier (EIN).

The final rule for the Transactions and Code Sets was published on August 17th, 2000. The compliance date for that rule is October 16, 2002. The final rule for the Privacy of Individually Identifiable Health Information was published on December 28th, 2000. The compliance date for the privacy rule is February 26, 2003. The final rules for the Security of Individually Identifiable Health Information, the National Provider Identifier, and the National Employer Identifier have not been published, but they are expected soon. The National Health Plan Identifier, Claims Attachments, and Enforcement are still under development.

The new Federal privacy regulations will affect you, in that you will have to modify internal policies and procedures, and document your privacy practices. You will also need to make sure that business relationships involving the exchange of personally identifiable health information include agreements for the protection of that information. Even if you do not use electronic systems to maintain health information, you are covered by the final Privacy rule. This was a significant change from the proposed rule, which had only covered health information in electronic form. The new Standards for Electronic Transactions final rule will impact you primarily in the areas of how you bill for services.

Privacy Regulation

Required Safeguards for Privacy of Protected Health Information

The HIPAA privacy regulation requires you to have appropriate administrative, technical and physical safeguards to protect the privacy of protected health information. These must protect the information from intentional or unintentional use or disclosure.

Medscape electronic medical record software products, including Logician, About My Health and our Internet EMR can help you with HIPAA compliance in this area in several ways:

- Audit trails for chart access
- Ability to designate sensitive documents
- Ability to designate sensitive charts
- Password protections
- Ability to set access based on individual user, or user's roles in Logician
- Ability to set access based on locations of care in Logician
- Release of information form handout in Logician
- Release of information encounter form in Logician
- Ability to flag a chart to indicate release of information restrictions in Logician
- Ability to add an addendum to a chart in Logician
- Secure Socket Layer (SSL)
- 128-bit or 256 bit encryption of data
- Ability to increase security for records that will be accessed via public computers

Medscape protects health information that we have access to in several ways. We use physical safeguards to protect health information that we have in our possession, or that we have access to. We have administrative policies and procedures designed to protect the confidentiality of health information. We provide our employees and contractors with privacy and security training. We

require authorization and biometrics identification in order for anyone to access our data center. We use fire walls, encryption, anti-virus software, and system back-ups to protect health information from destruction, alteration or misuse.

Covered Entities

The HIPAA standards apply to health plans, health care clearinghouses, and certain health care providers. Actions that are taken by business associates of a covered entity are considered to be the actions of the covered entity, under the Privacy rule. However, if there is a violation of a patient's privacy, the covered entity will only be penalized if they knew about a violation of privacy practices by the business associate and did not take any action in response to the violation.

Health Care

Healthcare is defined in the HIPAA Privacy regulation as "preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that effects the structure or function of the body and the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription."

Enforcement

A person who believes that you are not complying with the HIPAA requirements may file a complaint with the Secretary of Health and Human Services (HHS.) The Office for Civil Rights will enforce the HIPAA regulations. Both Civil and criminal penalties can result from non-compliance with the regulations.

Sanctions

You must have a process in place that provides for sanctions against members of your workforce for violations of your privacy policies and procedures.

Medscape employees are required to sign a confidentiality agreement regarding protecting the confidentiality of patient's health information. The agreement includes language that the employee may be terminated for violating the agreement.

What is Covered Under the Privacy Rule?

All individually identifiable health information in any form, electronic or non-electronic, that is in the possession of, or is transmitted by you is covered under the Privacy rule. Paper records that have never been electronically stored or sent are also covered. This is a change from the proposed rule.

Medical records, verbal communications about an individual, and billing records that are used by you to make decisions about a patient are included in the regulation.

Individually Identifiable Health Information

The regulations define “individually identifiable health information” as information that includes demographic information that is created by or received from a health care provider, health plan, employer, or health care clearinghouse. It is information related to the past, present, or future physical or mental health condition of a patient, the provision of health care to the patient, or the past, present, or future payment for the provision of healthcare. Individually identifiable information either identifies the individual, or is information for which there is reason to believe it could be used to identify the individual.

Protected Health Information

Protected health information is individually identifiable health information that is transmitted by electronic media, maintained in any medium, or transmitted in any other form or media. Electronic media includes Internet, Extranet, leased lines, dial-up lines, private networks, and magnetic tape, floppy disk or compact disk.

Consent VS Authorization for Release of Protected Health Information

Consents: You will have to obtain a general consent from the patient (except in emergency situations, or as required by law) in order to use or disclose protected health information for treatment, payment and healthcare operations. Consents are general in nature, and they must also refer the patient to your information practices policies. Consents only cover the specific covered entity, and do not allow re-disclosure of information to another entity. Patients may withdraw their consent to release information at any time, and the consent itself must tell them that they may do so.

Consents for releasing information must be written in plain language. A consent has to inform the patient that their protected health information may be used and disclosed by you to carry out treatment, payment, or healthcare operations. It

must refer the patient to your privacy practices policy. The consent must inform the patient of their right to request restrictions on uses and disclosures of their protected health information. It also must state that you are not required to agree to the request.

You are required to document and retain any signed consent for release of information that you receive from your patients for at least 6 years.

Authorizations: You have to get a written authorization from the patient to release their health information, except as permitted by law. These authorizations have to be specific and detailed permission to release protected health information for any reason other than for treatment, payment and healthcare operations. For example you would need to obtain a written authorization from the patient to send copies of their hospital History and Physical, Operative Report, and Discharge Summary to the patient's attorney. Exceptions to this requirement are when a patient requests copies of their own information, and when necessary for HIPAA regulation enforcement.

Authorizations must be written in plain language. An authorization must include a description of the information to be used or disclosed. An authorization must include the name or identification of the person that is authorized to use or disclose the information. It also must include the name or identification of the person to whom the entity is authorized to make the disclosure. The authorization must have an expiration date. It must state that the patient has the right to revoke the authorization in writing, and instructions about how to do that. It has to tell the patient that when information is disclosed, that it may be subject to re-disclosure by the recipient, and is no longer protected under law. The authorization has to contain the signature and date of signature of the patient. If a personal legal representative is signing the authorization, they must state their authority to act for the patient, (for example, because they are the legal guardian of the minor.)

Authorizations that are requested by a covered entity for their own use or disclosure can not condition treatment, payment, enrollment, or eligibility on the patient's authorization. These authorizations must say the purpose that the information will be used for. An authorization must tell the patient that they may inspect, or copy the information to be disclosed, and that they may refuse to sign the authorization.

Authorizations that will result in the covered entity receiving direct or indirect remuneration for the patient's health information, must include a statement that the remuneration will result, for example if you will receive a discount on a pharmaceutical company's products by providing the company with the patient's

demographic information in order for the company to directly market certain drugs to the patient, it must say so on the authorization form.

The protections for health information extend to deceased patients, and last for as long as you maintain the information. However, information about the patient may be released to coroners, medical examiners, and funeral directors without a signed authorization. If a person is a legally able to act as an executor or administrator of the individual's estate, they may be given access to the information about the patient, and they may authorize its release.

Minors who are able to consent to their own health care by law, are the individuals that you must ask for their consent or authorization to release protected health information from their records. This only applies to records that were created to document the treatment that they consented to on their own, (for example records of treatment given for venereal disease.)

Medscape's Logician product has a release of information form available as a patient handout that you can use when releasing patient's health information. There is also an encounter form to use to document what was released, whom it was released, when it was released, and the reason it was released.

Releasing Health Information Without Patient Authorization

You may use protected health information without patient agreement to help with notifying family members or others responsible for the individual's care, about the patient's general condition, location, or death. You may also disclose information to Federal, State, or local governmental agencies or private disaster assistance organizations for the purpose of disaster relief activities. You may release protected health information as permitted by law, health oversight, and for public health and Food and Drug Administration purposes without patient permission. This includes reporting of child abuse reporting, domestic violence, and other mandatory reporting laws and regulations.

Information may be disclosed without patient permission for national security and intelligence activities, protective services for the President of the United States, and medical suitability determinations for the Department of State for security clearance purposes.

You may disclose protected health information in a judicial or administrative proceeding if the disclosure is in response to a court order, or subpoena or summons issued by a court, grand jury subpoena, or with a discovery request form without patient permission. However, if a subpoena is not issued by a court,

you have to notify the patient of the subpoena, in order to allow him or her to object to the release of information. If the administrative request is not for information relevant and material to legitimate law enforcement inquiry and the request is not specific and is not limited in scope, and de-identified information could be otherwise used, you are not required to comply.

Protected health information that may be released to law enforcement without the patient's permission is limited to information necessary for them to identify and locate a patient that is a suspect, fugitive, material witness, or missing person or the date and time of their death. You may also release the name and address, date and place of birth, social security number, blood type, type of injury, date and time of treatment, date and time of death if applicable, and physical characteristics information to law enforcement. However, DNA information, tissue-typing analysis of body fluids or tissue, or dental records may not be released without the patient's permission. Information may also be released to avert serious threats to health or safety to another person.

You may release protected health information from deceased patient records to organ procurement organizations, and tissue banks.

Disclosures of protected information to law enforcement may be made to prevent threats to health or safety. However, it is not required. If the patient is a victim of a crime, you may give information to law enforcement if the individual agrees, or if you are not able to obtain the patient's agreement because they are incapacitated or due to emergency circumstances and under certain other circumstances.

Drug and Alcohol Treatment Records

The final HIPAA privacy regulation does not change the existing protections under Federal law for alcohol and drug treatment records. (See 42 USC 290dd-2 and 42 CFR part 2.) Under those protections, specific informed consent or a specific court order for those records is necessary in order for those records to be released, or even to acknowledge that you have those records.

Restrictions on Releasing Information

Patients may request restrictions on uses and disclosures of their own protected health information for treatment, payment or healthcare operations. However, you do not have to comply with the request. If you initially agree to the restriction, but later want to terminate the restriction, you can do that, with the agreement of the patient. However, if the patient disagrees with the change you want to make,

the agreement continues to apply to all information obtained prior to the initial agreement.

Restrictions on the use of protected health information can include asking you to send communications to the patient in a sealed envelope, or asking you to send particular information to the patient's work address rather than their home. The patient does not have to give a reason for the restrictions and you can not refuse the restrictions based on the perceived merits of the request.

You can flag a chart in Logician, and add information to the patient's chart saying that your patient wants the release of his or her information restricted.

Marketing

You will be able to communicate with a patient encouraging them to buy products or services that you are able to provide to the patient, and you may use protected health information to do that (for example. you may send a letter to all of your diabetic patients telling them about a diabetic foot clinic that the hospital will be offering.) The regulation treats this as part of healthcare operations, and excludes it from the consent requirement. However, if you are being paid to communicate with the patient for the purposes of advertising the new service, the patient's consent is necessary.

You must make the determination that the product or services that are going to be offered to the individual may be beneficial to the health of the class of patient targeted to receive the information. The communication sent to the patient must include information about how the patient can opt-out of receiving further communications about health related services. It must identify you as the party making the communication. The communication must state that you will receive direct or indirect remuneration for sending the communication, if you will be getting it. The communication must also tell the patient why they were targeted for the communication, and how the product or service relates to their health status or condition.

You may use demographic information and information about the dates of health care of your patients for the purposes of raising funds for your own office's benefit without getting the patient's consent. The fundraising materials must explain how the patient may opt-out of receiving any further fund raising communications.

Organized Healthcare Arrangement

An organized healthcare arrangement is one in which more than one covered entity participates in activities that require sharing of protected health information. It is one in which a patient expects that this sharing of information will occur, e.g. you provide healthcare to your patient while the patient is in the hospital. Both you and the hospital staff will need to communicate with each other about the patient. In this situation, the consent requirement does not apply.

Disclosure of Protected Health Information to Business Associates

You may disclose protected health information to a business associate only if you obtain satisfactory assurances that the business associate will handle the information appropriately. You will need to ensure that by getting them to sign a written contract. The contract must include language that the business associate will not use or disclose the information other than as the contract permits, or as required by law. The contract has to specify the permitted uses and disclosures, as well as to whom those disclosures may be made. It must say that appropriate safeguards to prevent use or disclosure of the information will be taken. The contract must require the business associate to be able to amend health information, and to provide an accounting of disclosures of the information that they may make. Disclosure may occur in order for the business associate to perform functions and activities for you. The contract may permit the business associate to provide data aggregation services for use in your healthcare operations.

You must take steps to fix known violations of the confidentiality of patient information, or terminate a contract with the business associate if those violations occur. If you know of a pattern of activity by the business associate that is a violation of the contract, and do not take action, then you will be considered to be in violation of the HIPAA requirements.

Business associates must destroy or return protected health information at the end of the contract with you. If that is not possible, the protections for the information must continue to be maintained for as long as the business associate keeps the information.

Medscape signs sales and other agreements and contracts with our customers and our business associates that includes language protecting the confidentiality of patient’s health information. Our policy is, not to release individually identifiable health information without the permission of the patient and physician.

Research

The rule defines research as a systematic investigation, including research development, testing and evaluation that is designed to develop or contribute to generalized knowledge. You have to obtain a patient's authorization for the use and disclosure of their protected health information that will be created for the purposes of research, and that includes the treatment of the patient.

A privacy board or Institutional Review Board (IRB) that has members of varying backgrounds must review the research protocol and its effect on the patient's privacy rights in order to approve of the use of protected health information. This board must include at least one member that is not affiliated with the covered entity conducting the research. The IRB may decide that releasing individually identifiable information without the patient's authorization is permissible because the research could not be conducted without it.

There needs to be an adequate plan to destroy the patient identifiers contained in the research data at the earliest opportunity, unless there is justification not to do so. The covered entity must get a written agreement from the person receiving the information that they will not re-disclose it. The chairman of the IRB must sign documentation stating that the above criterion has been met.

Protected health information may be used for research without patient authorization if de-identified information is used.

De-Identified Health Information

Health information is not considered identifiable if it does not identify the individual, or can not be used to identify the individual. Information is considered to be de-identified if the following are removed: name; geographic subdivisions smaller than a State including street address, city, county, precinct, zip code (except for the three initial numbers of the zip code, if the data contains more than 20,000 patients); telephone number; email address; social security number; medical record number; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers including license plate numbers; device identifiers and serial numbers; URL; IP address; biometrics identifiers including finger and voice prints; full face photographic images and comparable images; any other unique identifying number, characteristic or code. In addition, you must not know that the de-identified information could be used alone or in combination with other information to identify the patient.

You may assign a code to re-identify the patient if the code is not a derivative of some other information about the patient, and is not capable of being used to re-identify the patient, and if you do not disclose the method of re-identification to anyone else.

De-identified health information is not subject to the requirements of the privacy rule, unless it is re-identified.

Data Aggregation

Data aggregation is the combining of protected health information from many individuals to permit analysis that relate to your healthcare operations. Aggregated data is not protected under the HIPAA privacy regulation.

Correctional Facility Medical Records

While a patient is incarcerated, the correctional facility may use or disclose protected health information without patient authorization. Once the patient is released, the patient will have the same privacy rights as anyone else.

Policies and Procedures

You must have policies and procedures regarding the protection of protected health information from accidental or intentional use or disclosure and to protect against the inadvertent disclosure of protected health information to persons other than the intended recipient. The policy must safeguard the privacy and integrity of health information.

You must implement policies and procedures to identify the people or classes of people in your workforce that need access to protected health information in order to carry out their job duties. The policy must include the categories of information that an employee needs access to, and the conditions of that access.

Policies must be developed specifying that only the minimum necessary amount of protected information necessary to meet the purpose of the disclosure will be disclosed. This includes the minimum necessary information for your employees to accomplish their duties. The policy must state that an entire medical record will not be released except under specific circumstances.

Your policies and procedures must require the verification of the identity of the person requesting protected health information, if your staff does not already know the person requesting the information. The ability for you or your staff to legally comply with the request must also be verified.

A policy and procedure regarding patient's access to their own health information must be documented. Your policy must also specify who is authorized to determine when information will be withheld from a patient requesting access.

You must have a policy and procedure documenting the titles of the person or office responsible for receiving and processing requests for amendment.

You must have a policy and procedure regarding privacy training for members of your workforce. The policy must state that those individuals that have contact with protected health information will be trained regarding your privacy policies and procedures, and regarding protected health information. This training has to occur prior to the implementation date of the HIPAA privacy rule. The policy has to say that new employees will receive this training within a reasonable time after their date of hire. The policy must also state that as your privacy policies and procedures change, the employees will receive re-training.

You must have policies and procedures regarding how you will apply appropriate sanctions on members of your workforce for violations of your privacy policies and procedures.

You must modify your policies and procedures in a prompt manner in order to comply with changes in relevant law. When the changes also effect the privacy practices listed in the notice of privacy practices, you must also change the notice to reflect those changes.

You must keep documentation of these policies and procedures for a minimum of 6 years.

Medscape has policies and procedures regarding the protection of health information. These policies include policies requiring employees and contractors to receive privacy and security training, and designating which employees need access to health information based on their job duties.

Patient Right of Access to Health Information

Patients may request access to, and they are able to obtain a copy of their own record. The patient has the right to request that access for as long as you maintain the information. You may charge a fee for copying the records. However, the fee may only be for the cost of the materials used in making the copies, not for retrieving the information.

Patients do not have the right to access information from psychotherapy notes, information collected and used in civil, criminal or administrative proceedings, or

to get lab results directly from the laboratory without the you seeing the results first.

You will have 30 days to provide access to patients who request access to their own protected health information as long as the information is maintained on site. If the information is stored elsewhere, you must respond within 60 days.

You may deny patients requests to access their health information for several reasons, including:

- the information would endanger the life or safety of the patient or another person
- the information in their record is about another person and having the information would cause harm to the other person
- the information was obtained under promise of confidentiality
- the information was obtained as part of a clinical trial and the individual had agreed to denial of access when the trial was in process
- the information was collected for use in a legal proceeding
- the patient was an inmate in a correctional facility, (they may only have their access denied while they are incarcerated, and if that access would cause harm to another person;)

The denial of access must be given to the patient in writing. The denial letter has to explain in plain language the reason for the denial, and the patient's right to have the denial reviewed, as well as how the patient can disagree. Patients have the right to appeal the denial.

Patient's Request to Amend Protected Health Information

Patients have the right to request that their protected health information be amended for as long as you maintain the information. You must act on the patient's request within 60 days. You can deny the request if you did not create the information, if the information is accurate and complete, or if the information is not part of the record. You must notify the patient whether the request has been denied or accepted.

If the request is approved, the patient must approve the sharing of the amended information with entities that need the amended information. You must make the

appropriate amendment, or append the record or provide a link to the location of the amendment, if you have agreed to the amendment.

If the request is denied, you must send a denial letter that provides a reason for the denial, and explain how the patient may file a written disagreement, how they may make a complaint to your designated complaint staff, and how they can complain to the Secretary of Health and Human Services. You must also keep the patient's request, the denial of the request, the patient's letter of disagreement, and any rebuttal with the patient's original record.

You must permit the patient to submit a written statement disagreeing with the denial of their request for amendment. You may prepare a written rebuttal to the statement.

If you received a notice of amendment from another covered entity, you must make the necessary amendment to the information about the patient.

Logician allows you to add an addendum to a record, should a patient request an amendment.

Notice of Privacy Practices

Patients must be given a notice of privacy practices. If you only create or received protected health information as a business associate of other covered entities, you do not have to produce a notice.

The privacy practices notice has to be written in plain language. It has to describe: the uses and disclosures expected to be made without the patient's authorization. When the notice describes using the information for treatment, billing and healthcare operations, the notice has to provide at least one example of this type of use. The notice must include a statement telling the patient that information will not be released for any other purpose without their permission. It must inform the patient that they may revoke their permission to release information. The notice has to give information about the patient's right to request restrictions on the release of their information and that they have the right to inspect and obtain a copy their own medical record. It must state that they have the right to request corrections or amendments to their health information, and that they can request an accounting of disclosures of their information by you. The notice must state that the patient has the right to receive confidential communications from you. (For example, you are asked to send a pregnancy test result to the patient's work address, instead of their home address.) The statement must state that it is your responsibility to protect the patient's health

information. The notice has to state that the patient will be informed if these information practices change and how you will inform them. If you want to reserve the right to change your information privacy practices, you will need to include that fact in the notice.

The process for complaining about information practices and who to contact to register that complaint must be included in the notice of privacy practices, as well at that person's contact information.

The notice has to include the date the information practices notice was produced. It must include the statement that for all other uses of protected health information, the patient's authorization is required.

If you plan to contact the patient for appointment reminders, describing or recommending alternative treatments, providing health benefits and services that the patient might be interested in, or soliciting funds, you need to include that information in the notice.

The header of the privacy practice notice must read: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

Whenever your information practices or policies change, you have to change your notice of information practices as well, and you must revise each of the policies and procedures that apply.

If you want to be able to change your practices for the use of protected health information without having to segregate your records according to what notice was in effect at the time the records were created, you must reserve the right to do so in your notice of privacy practices. If you do not, you will have to separate the information obtained before a change in the notice from information obtained after the change in order to use it for the new purpose.

Your information practices notice must be posted in a prominent area of your office, clinic, pharmacy, or other location. You must provide the notice of privacy practices no later than the date of the first delivery of service to the patient. This requirement includes service delivered electronically.

If you have a Web site describing your services, you must make the privacy notice prominently available on the Web site. If the patient agrees to receive an electronic privacy notice, one may be sent. If the first service delivery to a patient occurs electronically, you must provide an electronic privacy notice automatically

after the patient's first request for service, e.g. the first time a patient uses an Internet pharmacy to fill a prescription, the pharmacy must automatically send the patient their notice of privacy practices.

Medscape has a privacy policy and terms of use policies for our Web-based products and services that specify how we will use health information. These policies are posted on our Web sites.

Accounting of Disclosures of Protected Health Information

Patients have the right to an accounting of all disclosures of their protected health information by you for purposes other than treatment, payment, and health care operations. You must provide a requested accounting no later than 60 days after receiving the request. The patient has the right to this accounting of this information for the previous 6 years. This accounting does not have to be provided if the information was disclosed for purposes of treatment, payment and healthcare operations. It does not have to include disclosures made for the purposes of national security or intelligence, disclosures to correctional institutions, or disclosures that were made by you prior to the compliance date of the rule. You must exclude disclosures to health oversight agencies or to law enforcement officials if requested to do so by the official, but for no longer than 30 days from the date of the request.

The accounting of disclosures must include:

- the date of the disclosure
- name of the person or entity that received the information and that entity's address
- a description of the information disclosed
- a brief statement of the purpose of the disclosure

Alternately, you must keep a copy of the patient's written request for disclosure, and/or a copy of the patient's authorization for disclosure.

Patients may receive one free accounting of disclosures every 12 months. After the first request in that year, you may charge a reasonable cost based fee.

You must keep documentation of any accounting of disclosure of protected health information that you have provided to a patient.

Logician contains an encounter form that allows you to record the above information regarding the release of health information. Reports may be written to retrieve that information for you. Additionally, we have audit trails that track chart accesses in Logician, and in our other EMR products.

Privacy Official and Contact Person

You must designate a privacy official. The privacy official must be responsible for the implementation and development of your privacy policies and procedures. You must document who your privacy official is, and who your contact person is for complaints regarding your privacy policies and practices. The contact person must be charged with dealing with complaints about privacy of their health information, and to provide information about your notice of privacy policies.

Medscape has a privacy official that is the Healthcare Compliance and Privacy Officer. This position is within the Legal Department at Medscape. We have contact information posted on our Web sites about how to contact the Healthcare Compliance and Privacy Officer and to register concerns about our privacy practices. That person may be contacted at *privacy@medscapeinc.com* .

Training

All members of your workforce that have contact with protected health information must be trained on your policies and procedures regarding protected health information. You must have provided this training to each of those employees before the effective date of the final privacy rule. New members of your workforce must be trained within a reasonable time after joining the workforce. Each time there is a material change in your privacy policies and procedures, you must provide training about those changes to your workforce. This training must be documented.

Medscape provides training regarding the privacy and security of health information to new employees and contractors at each new employee orientation.

Compliance Date

You must comply with the HIPAA privacy regulation no later than February 2003.

Standards for Electronic Transactions

Who Has to Use a Standard HIPAA Transaction?

In general, if you conduct a covered transaction with another covered entity, or within the same covered entity if you are part of a larger organization, you must conduct the transaction as a standard transaction. However, you may use a business associate to conduct an electronic transaction for you. Additionally, you may use direct data entry offered by a health plan to conduct transactions without using a standard transaction to enter that information.

Transactions include health care claims, health care payment and remittance advice, coordination of benefits, healthcare claim status, enrollment and disenrollment in a health plan, eligibility for a health plan, health plan premium payments.

Standard Code Sets

The standard code sets that HIPAA requires are:

- ICD-9CM for diagnosis coding,
- National Drug Codes (NDC) must be used for drugs and biologicals
- Code on Dental Procedures and Nomenclature must be used for dental services
- Health Care Financing Administration Common Procedural Coding System (HCPCS) and CPT-4 must be used for physician services and other health care services. HCPCS is the required code set for other substances, equipment, supplies and other items used in health care services.

Trading Partner Agreements

You will not be allowed to enter into a trading partner agreement that will do any of the following:

- change the definition or data element in a standard
- add any data elements or segments to the maximum data set
- use any code or data elements that remarks “not used” in the implementation specification

- change the meaning or intent of the standard's implementation.

Claims

You will have to use the following transaction standards in your office. You can get information about these standards at Washington Publishing Company *http://www.wpc-edi.com*

- ASC X12N 837 for submitting electronic health care, professional health care, and dental claims.
- ASC X12N 270/271 for eligibility benefit enquiry
- ASC X12N 278 for health care services review
- ASC X12N 276/277 for health care claim status request and response
- ASC X12N 835 for health care claim payment/advice
- NCPDP for retail pharmacy drug claims

Medscape's Use of the HIPAA Transaction Standards

Medscape uses ICD-9-CM to record diagnoses, and CPT-4 to record procedures and services within our electronic medical record products. We do not produce billing software, and so do not use the ASC X12N standards. We do not have a pharmacy product, and so do not use the pharmacy transaction standards.

Compliance Date

You must comply with the HIPAA transaction standards regulation no later than October 2002.

Conclusion

You will have to comply with the HIPAA regulations within two years. Using Medscape's electronic medical record software will help you become HIPAA compliant. However, much of the privacy regulation effects your own policies and procedures for protecting health information. You will need to develop and implement changes to these over the next two years to become HIPAA compliant.

The transaction standards will involve many software changes in how you transmit information for billing, claims, insurance coverage, and other transaction. The software vendors that supply tools that you use for these transactions should be contacted regarding how to make the necessary changes.