

INTRODUCTION

In 1996 the health care profession began hearing about HIPAA – the Health Insurance Portability & Accountability Act.

Many questions and misunderstandings began. Most doctors (hoped) they wouldn't be affected...but the truth is that *nearly all persons involved with health care* are mandated to comply with all rules & regulations.

The HIPAA rules & regulations are very complex, hard to understand and are published by the federal government. More than 7,000 pages of small print dictate a rule for nearly every conceivable action, transaction and mis-action which can and/or will occur in any providers office or hospital.

Even though the rules & regulations are hard to understand...they are not optional. Fines, penalties and worse will be enforced against any violators !

Due to lack of understanding and/or misinterpretations, many doctors failed to acknowledge and/or take the time to identify with deadlines....presuming that the deadlines didn't apply to them !

Today these same doctors have discovered that their failing to comply with certain deadlines has placed them in jeopardy. For example. The deadline for filing a HIPAA compliance plan was October 15, 2002. Considering that 90% of all doctors, hospitals and "covered entities" were not prepared and/or ready with their compliance plans the government provided a one-year extension for any provider just for by completing a simple questionnaire, which was easy and only took 5 minutes on-line.

Those who filed the simple on-line form received a federally assigned registration number which is to be published and printed on the individuals compliance plan program. Those with this number now have a one-year extension for claims processing. Those who didn't file their extension request are mandated today to be in complete compliance with all HIPAA rules & regulations.

Some professionals have the false understanding that if they do not file bills and/or insurance claims electronically, they are exempt from HIPAA. The truth is that computer transactions, on-or off line, are only a small part of the HIPAA rules.

**HIPAA PRIVACY RULE GUIDELINES
FOR THE PRIVATE PRACTITIONER PROVIDER**

One portion of HIPAA is *Privacy & Security*. Under HIPAA, every clinic and/or office must have a HIPAA privacy & security officer ! This officer may be the doctor and/or one or two people can hold these positions...but make no mistake...they are not optional even if the office is small and there is only 1 doctor and the spouse is the receptionist & sole employee.

The HIPAA Privacy & Security Officer positions require *written job descriptions, responsibilities, accountability and deadlines*.

The primary responsibility is for the Privacy & Security Officer to maintain & improve patient health information confidentiality, privacy, transmission and storage of data, which mean that job details include:

- ▶ Staff training, development & standards of operation
- ▶ Security & Privacy policies
- ▶ Procedures for intentional & unintentional violations
- ▶ Documentation programs
- ▶ Forms & Reports

Effective April 2003 all "covered entities" are required to comply with all *Privacy Rule guidelines* of HIPAA. The extension does not apply to the privacy rule...only the claim processing portion.

Please DO NOT ignore the HIPAA rules & regulations ! Non-compliance will be costly. Professional malpractice & liability insurance will not cover you for fines and/or penalties and the federal government will not accept *any excuses* for non-compliance.

This guideline will help you understand your responsibilities. HIPAA is just another change in the healthcare industry...flow with the change !

FUNDAMENTALS OF HIPAA – PRIVACY RULE

HIPAA... Health Insurance Portability & Accountability Act
Signed into law in 1996
Represents a wide set of far reaching health policy issues including:

- ▶ Health Insurance Access
- ▶ Health Care Reimbursement Fraud & Abuse
- ▶ Simplification of a variety of administrative tasks associated with health care services

The POWER of HIPAA...

Department of Health & Human Services (HHS) is authorized to develop standards and requirements for the:

- ▶ Maintenance & transmission of health care system by individual patients
- ▶ Improve the efficiency and effectiveness of health care systems by standardizing the interchange of electronic data for administrative & financial transactions
- ▶ Protect the security and confidentiality of electronic health information.
 - Adopt standards to facilitate health related financial transactions
 - Adoption of standards of vocabularies, terminologies and classification systems that name many of the diseases, procedures, medical problems, services and services encountered in the health care industry.

HIPAA regulate...

Covered entities, physicians, hospitals, providers, insurance plans and persons or companies who transmit, store and/or maintain health care information.

Health care providers must know...

- ★ HIPAA rules & regulations are not optional, flexible and are mandatory for all health care providers, entities and suppliers.

**HIPAA PRIVACY RULE GUIDELINES
FOR THE PRIVATE PRACTITIONER PROVIDER**

HIPAA has -7- key components...

1. Privacy standards
2. Security standards
3. Transaction & code sets
4. National provider identifiers
5. National employer identifiers
6. National health plan identifiers
7. Health claim attachments

Violations can result in....

- ▶ Monetary fines that can reach \$250,000
- ▶ Professional licensing restrictions and/or revocation
- ▶ Punishment and/or imprisonment of up to 10 years.

PRIVACY RULE

45 CFR – §160.00 – §164.00

Privacy Rule applies to...

- ▶ Health care providers*
- ▶ Health plans
- ▶ Health care clearinghouses (electronic billing/servicing companies)
- (*) Applicable health care providers are those who file electronic billing and/or fund transfers.
- (**) Privacy Rule does not apply to employers, life insurance companies, or public agencies that deliver social security or welfare benefits.

Privacy Rule creates...

- ▶ National standards to protect individuals medical records and other personal health information.

Privacy Rule means...

- ▶ Patients have more control of their personal health information
- ▶ The Rule sets boundaries on the use & release of health records
- ▶ Non-compliance is not acceptable & penalties are stiff
- ▶ Patients can have a full copy of their health care record at anytime
- ▶ Transmission of all information - oral, written, electronic and/or in any other means is protected under the Privacy Rule.

Effective Date

Privacy Rule was effective 14 April 2001. Covered entities, most health care providers and health plans are required to comply with the Privacy Rule as of 14 April 2003.

COPYRIGHT 2003 – USA – ALL RIGHTS PROTECTED

ALL FORMS OF REPRODUCTION OR DISTRIBUTION ARE PROHIBITED

DJR CONSULTING SERVICES, LLC – 2621 RAYMOND DRIVE – ST. CHARLES, MISSOURI 63301
1-800-334-6090 FAX - 636-946-7817

**HIPAA PRIVACY RULE GUIDELINES
FOR THE PRIVATE PRACTITIONER PROVIDER**

Consents & Responsibilities...

- ▶ Health care providers must obtain a specifically written consent from the patient *before* treatment and/or any care. This consent is good for the entire treatment of said patient and is not required to be renewed.
- ▶ The consent must be maintained as a integral part of the medical record for 6 years from the date it was last in effect.
- ▶ The consent must permit the health care provider to use and disclose protected health information to carry out treatment, payment and/or health care operations.
- ▶ The consent does not allow for any use and/or disclosure of any intentional and/or unintentional use or disclosure of protected health care information.
- ▶ Patient may revoke in writing the consent for privacy disclosure
- ▶ Patient may request restrictions in the privacy disclosure
- ▶ Legal custodians, parents and minors are mandated by individual state laws.

Private health care providers must...

- ▶ Train employees & verify competency on privacy rules. Document training and have each employee sign a form stating their attendance, responsibilities and accountability.
- ▶ Protect against violations of "oral communications" in your office in which a non-employee, patient, visitor or guest may unintentionally hear a covered entity discuss any PHI of a patient.
- ▶ Develop clear, straight forward privacy policies in your office
- ▶ Provide every patient a printed privacy rights & responsibilities
- ▶ Protect patient records from unauthorized use and/or disclosure
- ▶ Appoint an individual to be accountable for all privacy issues in your office and/or all rules, regulations, amendments, updates etc. as they are published.

Private health care providers are allowed to...

- ▶ Refuse treatment to any patient who refuses to provide a written consent for disclosure of PHI (private health information)
- ▶ Use PHI when attempting to collect payment for services rendered. This is applicable when discussing PHI to a health insurance carrier and/or third party payer provided the proper consent was obtained from the individual.

**HIPAA PRIVACY RULE GUIDELINES
FOR THE PRIVATE PRACTITIONER PROVIDER**

Safeguards in communications...

- ▶ Always speak softly and in a means so PHI is not heard by any unauthorized person(s).
- ▶ Avoid using a patients name in public and/or in any area which unauthorized person(s) may hear PHI
- ▶ Place computer screens to avoid unintentional and/or unauthorized viewing of PHI
- ▶ Secure all medical records containing PHI in locked file cabinets and/or a locked medical record storage room at all times when the office is unattended.
- ▶ Destroy all computer and/or electronic storage media prior to discarding and/or leaving your office or control.
- ▶ Protect transmissions of faxes from unauthorized viewing.
- ▶ Maintain all medical files with PHI during use to prevent unauthorized viewing.

Business Associates...

- ▶ Business Associates are independent contractors who may provide a function, service or activity to a covered entity where access to PHI may occur.
- ▶ Business Associates are required to sign a protective agreement before engaging in any services listed above.

Marketing & Public Relations...

- ▶ Providers may advertise services which are provided to patients
- ▶ Providers may not disclose patients names and/or identities in any form of marketing or advertising
- ▶ Providers may send reminders notices for appointments and/or periodic procedure(s) provided notices are sent in an sealed envelope.
- ▶ Providers must ensure that all forms of communications that may be considered marketing or public relations have the individuals authorization to use or disclose any PHI prior to creating and/or distributing the information.

Q&A

COMMONLY ASKED QUESTIONS & ANSWERS

1. Are sign-in sheets allowed under the HIPAA privacy rules ?
YES ! Physicians may use sign-in sheets but information revealed on the sheets must be necessary for daily operation and patient flow and cannot reveal any information considered unnecessary for the purpose of signing in at the reception desk.
2. Can we refer to a patient by name in the office and/or where other patients can hear their name announced.
YES ! It is considered appropriate to announce a patient's name while they have presented for care while in your office.
3. How can I fax and/or e-mail information about a patient without violating their privacy ?
You can transmit health related information electronically provided you have the patient's permission and/or have complied with safeguards such as preventing any unauthorized person from viewing the document prior and/or during transmittal and/or the transmission is directed to the selected receiver.
4. We have plastic chart holders outside the door of our treatment & exam rooms. Are these OK ?
YES ! You can have these holders but you must take appropriate measures to protect patient's privacy and not allow incidental disclosures to occur. It is suggested that you only provide name identification on the front side of the file and not both sides. Refer questions to 45 CFR § 164.530 (c).
5. Can I give a patient their file to carry to an assigned area in the office ?
YES ! You can give the patient their own file – but not anyone elses.
6. Can patients, visitors and/or family members wander around the office unattended?
NO ! Patients must be escorted to and/or directed to a treatment facility. Visitors and family members must be restricted to the reception room unless they are a minor and in the custody of a guardian or parent.

**HIPAA PRIVACY RULE GUIDELINES
FOR THE PRIVATE PRACTITIONER PROVIDER**

7. If I have a non-employee and/or outside business perform services in my office do I have to take any safeguards ?
YES ! You must have any contract laborer, outside agency and/or person sign a Business Agreement prior to engaging in any work and every year thereafter who will have access to protected health information?
8. What about other persons who do not normally have access to protected information and are not left unattended in any area where protected information is accessible?
Housekeeping staff, repair technicians, painters, plumbers, photocopy repair persons, carpenters etc. typically do not have access to protected health information therefore would not be required to sign a business associate agreement and any disclosure would be considered incidental disclosure.
9. If I use an electronic clearing house and/or outside billing service to process my insurance claims do I have to gain any specific authorization ?
YES ! A business associate agreement must be signed and on file to maintain confidential communications on all protected patient privacy information.
10. If a representative of a legal service bureau presents for photocopies of a medical record, am I required to have a business associate agreement on file ?
YES ! If they are gaining access to protected patient information.
11. If a patient requests photocopies of their medical file, am I required to give it to them if they still owe me money and/or can I charge for the record ?
YES...to all of the above. You are required to provide the record and you can charge a reasonable fee for actual services such as photocopying charges, staff time, handling and postage plus any provider time necessary for the preparation of any reports. Refer to 45 CFR § 164.524.
12. Can I release secondary information in a patients file which was received from another provider ?
YES ! If you have signed releases and/or document release from the originator of the documents – but if a document is marked “not for secondary release” you are prohibited from releasing said document.
13. If a violation of a patients rights occurs what action should and/or can be taken against the violator ?
Providing the action occurred after the deadline date, a complaint must be filed within 180 days of when the act occurred and/or was identified. Complaints are filed with the Office of Civil Rights. Refer to (www.hhs.gov/ocr/hipaa) to file complaints.

**HIPAA PRIVACY RULE GUIDELINES
FOR THE PRIVATE PRACTITIONER PROVIDER**

14. Is the deadline date for the privacy rule different for various providers and why?
YES ! The deadline for "covered entities" who are health care providers (including doctors and hospitals) complying with the privacy rule is April 14, 2003. Small health plans have until April 14, 2004.
15. Please explain the following term...
Incidental Disclosure – information that is released as a result of an otherwise permitted disclosure when provider has exercised reasonable & appropriate safeguards (45 CFR § 164.530 (b) (c) (d)).
16. We are using the same office forms for the past several years – can we still use them or must we change to new ones and if we must change when is the deadline and how do we know they are compliant?
Office forms may be used for many years provided they are compliant with all published rules and regulations. It is unlikely that any printed and/or published office forms available prior to the year 2000 are compliant. You are responsible for your office forms being compliant as of 4/15/03 and should only obtain forms from a reliable source aware of compliance issues.
17. Can we phone call a patient who missed an appointment and/or leave a message on a telephone recording machine?
NO ! You may not phone call any patient without the express written consent of a patient prior to the phone call taking place and you cannot leave any message other than your identity and a number where they can call you back.
18. Can we send post-cards, reminder cards and/or other mail which is not sealed in an envelope to a patient ?
NO ! All mail must be sealed in an envelope.
19. Can we publically post any appreciations, thank you for referrals and/or testimonials identifying a patients name in our office and/or any publication, newsletter or advertisement ?
NO ! All such are a violation of the protected information. A special release must be obtained prior to any such release.
20. Can I mention a patient's name and/or condition to any other patient, even if I know they are good friends and/or a relative.
NO ! All such information about a patient is private health & protected.

**HIPAA PRIVACY RULE GUIDELINES
FOR THE PRIVATE PRACTITIONER PROVIDER**

21. If my staff were to violate a patients privacy can I be held responsible and can my staff face the same or similar fines, penalties and/or punishment?
YES ! You are responsible for all actions and/or violations of all employees and your staff will be held to the same standards as any professional provider and staff may be responsible for their own fines, penalties and punishment.
22. Are all doctors and staff required to attend a HIPAA privacy rule seminar?
NO ! Authorities do not care where you learn about rules and regulations but all doctors and staff are required to comply with all HIPAA privacy rules and regulations as of 15 April 2003.
23. Are older or disabled doctors or staff exempt from being required to know and comply with privacy rules and standards ?
NO ! Everyone who is considered a covered entity must be in compliance.
24. Are the penalties, fines and punishment varied depending on the severity of the violation ?
Penalties, fines and punishment are very strict and costly. One could expect fines can exceed \$25,000 and punishment can include incarceration.
25. Will the HIPAA rules and regulations change and how do I keep up with revisions?
YES ! Updates are released periodically by the OCR and/or federal agencies. Covered entities are required to maintain current awareness via any means available. Rules and regulations are published by governmental agencies with ready access to providers.