Health & Safety Exemption Requirement

Auburn Montgomery adheres to all requirements pertaining to the protection of student information. Information about Student Records and confidentiality can be found online at http://www.aum.edu/ferpa.

However, there are limited exceptions to FERPA regulations under which Auburn Montgomery is permitted to disclose education records or personally identifiable, non-directory information from education records in connection with a health or safety emergency without student consent.

The situation must present imminent danger to a student, other students, or members of the school community in order to qualify as an exception. This action is not taken lightly and only under circumstances that present imminent danger.

Summary of HIPAA Privacy Rule

HIPAA is a federal law that gives you rights over your health information and sets rules and limits on can look at and receive your health information.

Your Rights

You have the right to:

- Ask to see and get a copy of your health records.
- Have corrections added to your health information.
- Receive a notice that tells you how your health information may be used and shared.
- Decide if you want to give your permission before your health information can be used or shared for certain purposes, such as marketing.
- Get a report on when and why your health information was shared for certain purposes.
- If you believe your rights are being denied or your health information isn't being protected, you can:
    - File a complaint with your provider or health insurer, or
    - File a complaint with the U.S. Government.

You also have the right to ask your provider or health insurer questions about your health rights. You can also lean more about your rights, including how to file a complaint from the Web site at www.hhs.gov/ocr/hipaa/ or calling 1-866-627-7748.

Who Must Follow this Law?

- Doctors, nurses, pharmacies, hospitals, clinics, nursing homes, and many other healthcare providers
- Health insurance companies, HMOs, most employer group health plans
- Certain government programs that pay for healthcare, such as Medicare and Medicaid

What Information is Needed?

- Information your doctors, nurses, and other healthcare providers put in your medical record
- Conversations your doctor has had about your care or treatment with nurses and other healthcare professionals
- Information about you in your health insurer's computer system
- Billing information about you from your clinic/healthcare provider
- Most other health information about you, held by those who must follow this law

Providers and health insurers who are required to follow this must keep your information private by:

- Teaching the people who work for them how your information may and may not be used and shared
- Taking appropriate and reasonable steps to keep your health information secure

To make sure that your information is protected in a way that does not interfere with your healthcare, your information can be used and shared;

- For your treatment and care coordination
- To pay doctors and hospitals for your healthcare
- With your family, relatives, friends or other you identify who are involved with your healthcare or your healthcare bills, unless you objects
- To protect the public's health, such as reporting when the flu is in your area, or
- To make required reports to the police, such as reporting gunshot wounds

Your health information cannot be used or shared without your written permission unless this law allows it. For example, without your authorization, your provider generally cannot:

- Give your information to your employer
- Use or share your information for marketing or advertising purposes
- Share private notes about your mental health counseling sessions

Auburn Montgomery Student Health Services
Employee Reference Regarding HIPAA Laws

HIPAA PRIVACY RULE – WHAT EMPLOYERS/EMPLOYEES NEED TO KNOW

One of the most important aspects of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is its privacy protection. The law gave the U.S. Department of Health and Human Services the responsibility of adopting rules to help patients and other health care consumers keep as much of their personal information private as possible. The HIPAA privacy rules has been in effect since 2003 for "covered entities," and even though employers are generally not covered entities, they are definitely affected by the rules applying to entities that are covered. The HIPAA privacy rule Web site from HHS (www.hhs.gov/ocr/privacy/) has much guidance on the rule. Including a very lengthy Q & A section that attempts to cover the privacy rule from the standpoint of covered entities, employers, health care consumers, health care providers, and other interested parties.

This article presents basic information about the HIPAA privacy rule in question and answers format and is specifically focused on the most important things that employers need to know about how the privacy rule will affect them.

What is the primary purpose of the HIPAA privacy rule?

The rule protects from unauthorized disclosure of any personally identifiable health information (protected health information, or PHI) that pertains to a consumer of health care services.

What is considered "personally-identifiable health information"?

Health information is considered to be personally identifiable if it related to a specifically identifiable individual; under 45 C.F. § 160. 103, it generally includes the following, whether in electronic, paper, or oral format:

1. Health care claims or health care encounter information, such as documentation of doctor's visits and notes made by physicians and other provider staff
2. Health care payment and remittance advice
3. Coordination of health care benefits
4. Health care claim status
5. Enrollment and disenrollment in a health plan
6. Eligibility for a health plan
7. Health plan premium payments
8. Referral certifications and authorization
9. First report of injury
10. Health claims attachments
11. Health care electronics funds transfers (EFT) and remittance advice
12. Other transactions that HHS may prescribe in future regulations

What is a covered entity?
The privacy rule applies to health plans, health care clearinghouses, and health care providers. It applies to employers only to the extent that they somehow operate in one of more of those capacities. The same standards apply to covered entities in both the public and private sectors.

How might an employer be a covered entity?
Normally, an employer will only deal with covered entities, not actually be one. However, if an employer has any kind of health clinic operations available to employees, or provides a self-insured health plan for employees, or acts as the intermediary between its employees and health care providers, it will find itself handling the kind of PHI that is protected by the HIPAA privacy rule.

What must covered entities do to project consumers of health care?
Covered entities must adopt written PHI privacy procedures; designate a privacy officer; require their business associates to sign agreements respecting the confidentiality of PHI; train all of their employees in privacy rule requirements; give patients written notice of the covered entities' privacy practices and access to their medical records; a chance to request modifications to the records; a chance to request restrictions on the use or disclosure of their information; a chance to request an accounting of any use to which the PHI has been put; and a chance to request alternative methods of communicating information. They must also establish a process for patients to use in filing complaints and for dealing with complaints. Finally, they must take any measures necessary to see that PHI is not used for making employment or benefits decisions, marketing, or fundraising.

What do the written privacy procedures include?
A covered entity's written privacy procedures must include safeguards for administration of PHI, physical security of such information, and electronic and other types of technical security. The procedures should include the designation of a privacy officer and an explanation of the complaint and resolution process.

When is patient authorization necessary?
Under 45 C.F.R. § 164.506(c), patient authorization is not necessary if a disclosure is made for purposes of treatment, securing payment, or in accordance with the operations of a health care provider. If PHI is to be disclosed for any other purpose, the patient's written authorization is mandatory.

When disclosing PHI, what must a covered entity do?
Whether the PHI must be authorized or does not need to be authorized, the covered entity must always release only as much information is necessary to address the need of the entity requesting the information (what the regulation refers to as the "minimum necessary" information to satisfy the inquiry).

What penalties apply to violations of privacy rule requirements?
There are civil penalties of $100 per violation, but the penalties can be "stacked" if there are multiple violations with respect to a single individual. The maximum civil penalties are $25,000 per year, per person, per standard. Thus, if two standards were violated with respect to one person, the potential penalties could mount to as much as $50,000. Criminal penalties (up to a $250,000 fine and ten years in prison) may be imposed for "knowingly and improperly" disclosing information or obtaining information under "false pretenses", with higher penalties reserved for violations designed for financial gain or "malicious harm". In addition, of course, state laws may impose additional penalties for the same offenses, and most states would also allow common-law suits for torts such as invasion of privacy and infliction of emotional distress, among other causes of action. In November, 2004, a federal district court sentenced a former employee of a Seattle, Washington cancer clinic to 16 months in prison under tile criminal penalty provisions of HIPAA after he admitted he used a patient's birthdate and SSN information to fraudulently obtain four credit cards in the patient's name and charge over $9,000 in goods.

Are there any exceptions to the privacy rule?
It is possible to disclose PHI without authorization if there is a compelling need for disclosure, such as when the information is needed for public health situations, court and agency proceedings (such as workers' compensation claim proceedings- see below), agency requirements (such as OSHA 300 logs- see OSHA Standards Interpretation Letter, August 2, 2004, http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=INTERPRETATIONS&p_id=24898), law enforcement, emergencies, identification of deceased people, and national security-related situations (see 45 CFR § 164.512(a, e, and 1)).

OSHA Logs and HIPAA
In an OSHA Standards Interpretation letter dated August 2, 2004, OSHA held that the HIPAA privacy rule does not require employers to remove names of injured employees from the OSHA 300 log. This is due to the exception under HIPAA for records that are required by law. Since the OSHA 300 log is a required record, employers have no choice but to include all necessary information on it, including the employees' name and injury information. See the OSHA letter at the following address: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=INTERPRETATIONS&p_id=24898

Workers' Compensation and HIPAA
There is no problem with employers, workers' compensation insurance carriers, physicians, and other participants in the workers' compensation system sharing protected health information with each other in connection with workers' compensation claims and appeals. HIPAA specifically allows three exemptions for workers' compensation-related matters:

1. if the disclosure is "[a]s authorized and to the extent necessary to comply with

laws relating to workers' compensation or similar programs established by law that provide benefits for work-related injuries or illness without regard to fault." 45 C.F.R. § 164.512(1).

2. if the disclosure is required by state or other law, in which case the disclosure is limited to whatever the law requires. 45 C.F.R. § 164.512(a).
3. if the disclosure is for the purpose of obtaining payment for any health care provided to an injured or ill employee. 45 C.F.R. § 164.502(a)(1)(ii).

Thus, the employee's written authorization is not necessary for the disclosure if one of those exceptions applies, and the employee also would not be able to require the covered entity to withhold the information under 45 CFR § 164.522(a). The bottom line is that if any health-related information is being exchanged in conjunction with a workers' compensation claim or appeal, the HIPAA privacy rule will not stand in the way. For a useful brochure on this subject from the Texas Department of Insurance's Workers' Compensation Division, go to http://www.tdi.texas.gov/wc/news/advisories/documents/hipaa-faq.pdf (PDF) on TDI's Division of Workers' Compensation Web site.

What about state laws?

The HIPAA privacy rule establishes a national minimum standard. If a state law provides greater privacy protections, the state law must be observed. As it happens, the equivalent Texas state law (Texas Health and Safety Code, Chapter 181 - online at http://www.twc.state.tx.us/news/efte/hipaa_basics.html), applies to more types of entities, requires consent for treatment, and otherwise provides similar protections. Since the Texas law defines "covered entity" as anyone who has any role at all in the production, gathering, storing, processing, or transmittal of PHI, as well as anyone who comes into possession of such information, some have argued that any employer who finds out or stores information relating to the medical condition of employees is covered under the law. However, the same state law provides that employers are not covered entities except with respect to re-identification of protected health information and use of PHI for marketing purposes (Texas Health & Safety Code, Section 181.051 (3)). Nevertheless, Texas employers and their employees should be careful in how they deal with medical privacy issues in their workplaces. The regulations adopted by the Texas Department of Insurance for medical information privacy provide some guidance (28 T.A.C. Part 1, Chapter 22, Sub chapter B). The exceptions for covered entities are found in TDI rule 28 T.A.C. § 22.57. However, since there have been no court decisions issued yet under that 2001 law or the regulations, employers should seek the guidance of qualified legal counsel if they have an unusual medical information privacy issue. The general wisdom applies here: when in doubt, keep the information as private and confidential as possible, and ask for the affected employee's written authorization to release it (to obtain a HIPAA-compliant waiver from employees, engage private counsel experienced in HIPAA issues- this is no area for a non-specialist).

Reference: http://www.twc.state.tx.us/news/efte/hipaa_basics.html

Student Health Services
HIPAA Confidentiality Agreement

Employees and students will have access to confidential information, both written and oral, in the course of their employment and job responsibilities. It is imperative that this information is not disclosed to any unauthorized individuals to maintain the integrity of the patient information. An unauthorized individual would be any person that is not currently an employee of the practice or student in training with the Nurse Practitioner. Any other disclosures may only occur at the direction and with written permission by patient.

I have read and understand the practice's policies with regards to privacy and Security of personal health information. I agree to maintain confidentiality of all information obtained in the course of my employment including, but not limited to, financial, technical, or propriety information of the organization and personal and sensitive information regarding patients, employees, and vendors. I understand that inappropriate disclosure or release of patient information is grounds for termination.

Signed: _____

Date:_____

AUM Student Health Services
Medical Information Release Form
(HIPAA Release Form)

Name: _____
Date of Birth: _____/____/_____

Release of Information

[ ] I authorize the release of information including the diagnosis, records; examination rendered to me and claims information. This information may be released to:

[ ] Spouse_____

[ ] Child(ren)_____

[ ] Other_____

[ ] Information is not to be released to anyone.

This Release of Information will remain in effect until terminated by me in writing.

Messages

Please call [ ] my home [ ] my work [ ] my cell Number:_____

If unable to reach me:

[ ] you may leave a detailed message

[ ] please leave a message asking me to return your call
_____

The best time to reach me is (day)_____
between (time)_____

Signed: _____
Date: ____/____/____

AUM Student Health Services
PATIENT HIPAA CONSENT FORM

I understand that I have certain rights to privacy regarding my protected health information. These rights are given to me under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). I understand that by signing this consent I authorize you to use and disclose my protected health information to carry out:

- Treatment (including direct or indirect treatment by other healthcare providers involved in my treatment);
- Obtaining payment from third party payers (e.g. my insurance company);
- The day-to-day healthcare operations of your practice.

I have also been informed of and given the right to review and secure a copy of your *Summary of the HIPPA Privacy Rule*, which contains a more complete description of the uses and disclosures of my protected health information and my rights under HIPAA. I understand that you reserve the right to change the terms of this notice from time to time and that I may contact you at any time to obtain the most current copy of this notice.

I understand that I have the right to request restrictions on how my protected health information is used and disclosed to carry out treatment, payment and health care operations, but that you are not required to agree to these requested restrictions. However, if you do agree, you are then bound to comply with this restriction.

I understand that I may revoke this consent, in writing, at any time. However, any use or disclosure that occurred prior to the date I revoke this consent is not affected.

Signed this _____day of _____ 20_____.

Print Patient Name _____

Signature _____

Relationship to Patient _____