

Privacy & Data Protection Update



Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

August 2009 - Issue 10

What's
Inside?

Medical Records Process — Revisited
The Difference Between Privacy & Security
Requests From Law Enforcement
Request for Amendment

Transporting Sensitive Information
Short URLs May Be Risky
FAQ: May I Fax Records To Other Offices?
Privacy & Security News

Requests for Medical Records Process — Revisited

Since the dissemination of the Registered Agent Policy, there has been some confusion with respect to how to process requests for medical records. All requests for medical records do **NOT** need to be sent to the Office of Medical Risk Management and/or to the Office of the General Counsel for review.

Requests for medical records must be fulfilled using a HIPAA-compliant request form or UHealth HIPAA Attachment 19 or 46. The Authorization Checklist will assist you in determining whether a request should be fulfilled by the department receiving the request. All multi-departmental/facility requests should be promptly provided to the Office of HIPAA Privacy & Security for processing and gathering of records.

Attorney letters should be processed in the same manner as outlined above and a copy of the request should also be faxed to Medical Risk Management, to the attention of Francesca Vallejo at 305-243-1404.



Related Links

- **Authorization Checklist:**
<https://www.med.miami.edu/hipaa/private/documents/auth3rdpartydisclosure.pdf>
- **Registered Agent Policy:**
http://www.miami.edu/policies_procedures/General-Business/PDF-Policies/BSF-080.pdf
- **Attachment 19 - Request for Access to Health Information:**
<https://www.med.miami.edu/hipaa/private/documents/D3900018E.pdf>
- **Attachment 46 - Authorization for 3rd Party Disclosure:**
<https://www.med.miami.edu/hipaa/private/documents/D3900052E.pdf>
- **All HIPAA Forms, including versions in Spanish and Creole:**
<https://www.med.miami.edu/hipaa/private/x53.xml>

The Difference Between the Privacy and Security of Health Information

Privacy is defined as a person's right to keep his/her individual health information from being disclosed without authorization. Privacy encompasses controlling who is authorized to access patient information and under what conditions patient information may be accessed, used, or disclosed to a third party. The HIPAA Privacy Rule applies to all protected health information (PHI).

Security is defined as the mechanism in place to protect the privacy of health information. This includes the ability to control access to patient information, as well as to safeguard patient information from unauthorized disclosure, alteration, loss, or destruction. Security is typically accomplished through operational and technical controls. Since so much PHI is now stored and transmitted by computer systems, the HIPAA Security Rule was created to specifically address electronic protected health information. As we move towards electronic health records and the digitalization of healthcare systems, information security and privacy practices become paramount.

Information security is the process by which privacy is achieved.

Frequently Asked Questions

Q: May medical information be faxed to another physician's office?

A: Yes, however, the fax number must be confirmed with the recipient prior to sending and the UHealth Fax Cover Sheet with the prescribed disclaimers must be used when sending faxes containing PHI or other sensitive information. If using pre-programmed numbers, periodically verify that the numbers are still correct.

Learn more and download the fax cover sheet at

<http://www.med.miami.edu/hipaa/public/x408.xml>

One-on-One Training

The Office of HIPAA Privacy & Security provides one-on-one and small group training specifically related to release of information and other related topics. To schedule a session, please contact our office at

Have a Question?

hipaaprivacy@med.miami.edu

Prior newsletters available online
<http://www.med.miami.edu/hipaa>

Requests from Law Enforcement

All requests from law enforcement must be received in writing on official letterhead. Should your department receive an inquiry regarding patient information from law enforcement, including the FBI or any other government agency, via telephone or in writing, please notify the Office of HIPAA Privacy & Security (OHPS) at 305-243-5000 and refer them directly to us for assistance.

When information is released, such requests must be accounted for in accordance with our HIPAA policies and federal law using an Attachment 45 - Accounting for Disclosures. This document must be completed by the employee disclosing the information and the written request must be attached. Both documents must then be sent to OHPS for scanning into the central repository.

A form titled "Attachment 45 - Accounting for Disclosures" from the University of Miami Miller School of Medicine. It includes fields for patient name, date of birth, and a table for recording disclosures. A barcode is visible at the bottom.

Related Links

- **Attachment 45 - Accounting for Disclosures:**
<https://www.med.miami.edu/hipaa/private/documents/D3900048E.pdf>

Requests for Amendment of Health Information (Attachment 33)

If a patient indicates there is an error in his/her medical record that needs correction, the patient should be provided an Attachment 33 - Request for Amendment of Health Information and the phone number for the Office of HIPAA Privacy & Security (OHPS). The patient should also be instructed to send the completed form to OHPS for processing. Should the form be received by a department, it should be forwarded to our office immediately. OHPS will facilitate the request for revision with the physician and communicate the granting or denial of the amendment directly with the patient.

By policy and regulation, the institution must respond to these requests within 30 days. All requests are processed by OHPS. For more information, please refer to the University's policy for Patient Amendment of Designated Record Sets.

Two forms side-by-side. The left one is "Attachment 33 - Request for Amendment of Health Information" and the right one is "Attachment 33 - Request for Amendment of Health Information" with a table for listing amendments. Both include patient information fields and a barcode.

Related Links

- **Attachment 33 - Request for Amendment of Health Information:**
<https://www.med.miami.edu/hipaa/private/documents/D3900031E.pdf>
- **University policy for Patient Amendment of Designated Record Sets:**
https://www.med.miami.edu/hipaa/private/documents/ppp_amendment.pdf

Transporting Medical Records and Other Sensitive Information

Medical records and other sensitive information are sometimes transported from one location to another, such as when moving to a new office, closing a location, etc. Here are some tips to help you protect this sensitive information during transit:

- Medical records and other sensitive information should not be left in an unlocked room or insecure area. Only authorized personnel should have access.
- All boxes containing medical records or other sensitive information should be numbered and appropriately labeled so as not to misplace them. Contents of the boxes should be logged and inventoried.
- Records should never be left unattended, even temporarily, including on pavements or in front of buildings or in hallways.
- An administrator should supervise all aspects of a move to ensure that the movers are aware of exactly what needs to be transported and proper, secure handling of sensitive information at all times during transit.
- Once the records have been moved to the new location, immediately make sure all items are accounted for, and again, store the information securely.

Should there be an incident where records or other sensitive information is lost, stolen, or accessed inappropriately, please notify the Office of HIPAA Privacy & Security as soon as possible.

Related Links

- **More information about Transporting Medical Records:** <http://www.med.miami.edu/hipaa/public/x378.xml>

Short URLs May Be More Than You Bargain For

Social networking sites, especially text-limited Twitter, have boosted the use of *short URLs*, web redirects that fit better in short messages. You might see an advertisement pointing to TinyURL.com, a status update linking to bit.ly, or a friend raving about a new restaurant with a link to snurl.com or some other short URL provider. Most providers search blacklists to block harmful links, but relying on their technology and not your own Internet savvy to protect you could actually put you, your computer, and all its sensitive information at risk.

The risk relies on the transference of trust. If a friend posts a link to a website, as long as you trust your friend, you are inclined to trust that the link is safe. When you visit <http://miami.edu>, you know the University of Miami is responsible for the content therein. If you trust the University, you will not worry about visiting the site.

When the use of social networking sites intersects with short URLs, however, the prudence of that trust decays and the risk increases exponentially. Sites like Facebook and Twitter encourage people to relay messages, re-post, re-tweet, etc. In that situation, your friend may not have taken the time to verify the link's safety.

Since the short URL masks the real destination, when you see one, you do not know where it leads. Without clicking the link, you would not know that <http://bit.ly/ZW7z5> loads the OHPS website listed at the bottom of this newsletter. Nothing within that URL assures you it will not install spyware on your computer or display inappropriate content. You cannot trust it.

Making matters worse, as we use legitimate short URLs more and more, we develop a new trust for them. Unless we remain consciously aware of the risk, this makes future attacks using short URLs easier.

Fortunately, you can avoid the malware that be found on untrusted sites (and the trouble that comes with it) by using tools like UnTiny.com and PrevURL.com that show you the real webpage behind the mask. Just copy the link and paste it into one of those sites, or install their browser plug-in to make it even easier to protect yourself and the information on your computer.

As always, your best defense is a good sense of online security. Avoid visiting or clicking on links from people you do not know. Use appropriate browser security settings and keep your software up-to-date with all relevant security fixes.

PRIVACY & SECURITY NEWS

Kaiser Fined for "Octomom" Privacy Violations

The California Department of Public Health fined Kaiser Permanente \$250,000 for violating patient privacy laws after hospital employees inappropriately accessed medical records for octuplet mother Nadya Suleman. Kaiser spokesman Jim Anderson said the hospital did not expect the reprimand, noting that Kaiser reported the violations to the state in February and punished nearly two dozen employees. A state report said 21 employees and two physicians inappropriately accessed Suleman's files. All were disciplined, including 15 who were fired or forced to resign.

"Medical privacy is a fundamental right and a critical component of quality medical care," said Dr. Mark Horton, the Department's director. "We are very concerned with violations of patient confidentiality."

TJX Settles Data Breach for \$9.75 Million

TJX, which operates more than 2,500 outlets nationwide, agreed to pay \$9.75 million to settle investigations by 41 state attorneys general, who were looking into the monster data breach, announced in January 2007, which exposed as many as 94 million credit and debit card numbers.

"This settlement ensures that companies cannot write off risk of a data breach as a cost of doing business," stated Massachusetts Attorney General Martha Coakley, whose office took the lead on the investigation. "In addition to the monetary relief, this agreement requires TJX to implement and maintain a substantial data security program to ensure that this kind of data breach does not happen again."

Boxes of Medical Records Found in Salt Lake Dumpster

KUTV in Utah reports that about 20 boxes of medical records were found in a dumpster. The files contained names, credit card numbers, Social Security numbers, canceled checks, routing numbers, and medical information. At least some of the records appeared to come from Mountain Medical Center. It was also reported that surveillance video showed two people drove up in a red pickup truck and unloaded the materials from a trailer. Salt Lake Police packed away almost twenty boxes of papers and said they would protect the documents as they dug into the matter.

Related Links

- **Kaiser @ HealthImaging.com:** http://www.healthimaging.com/index.php?option=com_articles&view=article&id=17471
- **TJX @ Law.com:** <http://www.law.com/jsp/article.jsp?id=1202431740322>
- **Salt Lake @ Connect2Utah:** <http://connect2utah.com/content/fulltext/?cid=37249>