The HIPAA Privacy Rule permits physicians to disclose protected health information to another healthcare provider for treatment purposes without patient authorization. For example, if a provider from Mercy or Baptist Health System is requesting records for treatment purposes, the request must be submitted in writing, on letterhead. Once the request is received and we have gathered the records, we can send records by fax or by mail. If records are sent by fax, notify the recipient to expect the fax. Staff must use the prescribed cover sheet whenever faxing health or other sensitive information. To request records from outside providers, use the Provider to Provider Release for Treatment form. If you have issues obtaining the records, contact our office for assistance at 305-243-5000.

**Related Links**
- **Business Associates Web Form**: http://www.med.miami.edu/hipaa/public/x243.xml
- **More on Business Associates**: http://www.med.miami.edu/hipaa/public/x442.xml

**Important Subpoena Tip**
If you are asked to release protected health information based on a subpoena, remember that all subpoenas must be HIPAA-compliant before any PHI is released. Please refer to the Subpoena Quick Reference Guide to make certain before proceeding with the release. **Remember**: By law and policy, we are required to account for Disclosure using Attachment 45 for all information released in response to a subpoena.

**Related Links**
- **Subpoena Quick Reference**: https://www.med.miami.edu/hipaa/private/documents/SubpoenaQuickReference.pdf
- **Attachment 45 — Accounting for Disclosure**: https://www.med.miami.edu/hipaa/private/documents/D3900048E.pdf

**Releasing & Requesting Records for Treatment**
The HIPAA Privacy Rule permits physicians to disclose protected health information to another healthcare provider for treatment purposes without patient authorization. For example, if a provider from Mercy or Baptist Health System is requesting records for treatment purposes, the request must be submitted in writing, on letterhead. Once the request is received and we have gathered the records, we can send records by fax or by mail.

If records are sent by fax, notify the recipient to expect the fax. Staff must use the prescribed cover sheet whenever faxing health or other sensitive information. To request records from outside providers, use the Provider to Provider Release for Treatment form. If you have issues obtaining the records, contact our office for assistance at 305-243-5000.

**Related Links**
- **Fax Cover Sheet**: https://www.med.miami.edu/hipaa/private/documents/um_hipaa_fax_cover3.doc
- **Provider to Provider Release of Information for Treatment Purposes**: https://www.med.miami.edu/hipaa/private/documents/pprtp.pdf
Two new rules were created requiring healthcare organizations and other entities that interact with personal health records to issue notifications in the event of a data breach. Both rules were created as part of the American Recovery and Reinvestment Act of 2009 (ARRA).

An interim final rule, issued by the U.S. Department of Health and Human Services (HHS), requires healthcare organizations subject to HIPAA regulations to notify individuals whose information has been breached, when the breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals must be reported to HHS annually. The rule also applies to business associates of healthcare organizations.

"This new federal law ensures that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care," Robinsue Frohboese, acting director and principal deputy director of the HHS Office for Civil Rights, said in a statement. "These protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information." Learn more.

Related Links

- SC Magazine — Health care breach notification mandated:
All I Need to Steal Your Identity, I Learned from Facebook & MySpace

It's easy to join social networking sites like Facebook and MySpace. A friend or coworker might have already sent you an invitation.

However, with the good also comes the bad. The popularity of social networking sites have made them objects of increasing attention from hackers and spammers. Remember that any information you post may be completely public and available to individuals who are most definitely not your friends. While the level of personal information you choose to share is your choice, posting of any sensitive work-related information is a definite no-no.

Related Links
- Security Awareness Tip: http://www.med.miami.edu/hipaa/public/x430.xml

Privacy & Security News

Houston Hospital Workers Fired for HIPAA Violations
Sixteen workers were fired from the Harris County Hospital District in Houston, Texas, for alleged violations of patient privacy laws. The incident involved the records of a first-year resident of the Baylor College of Medicine. The fired employees included managers, nurses, clerks, and other employees. A county employee who requested anonymity said hospital administrators told him at least a dozen employees not involved in the resident's care also looked at her records. "[T]he district wants to draw a hard line against any violations of the law in order to discourage the federal Office of Civil Rights from imposing large civil or criminal financial penalties," said Stacey Tovino, a professor of health law at Drake University.

Personal and Medical Information Breach — 1.5 million records
Health Net, one of the nation's largest publicly traded managed healthcare companies, confirmed that 1.5 million patients' records with medical claims and other data — spanning seven years — were included on a missing computer hard drive. The hard drive also included physician billing details such as tax ID numbers and patient diagnosis information. The insurer spent six months doing a forensic investigation to determine what data was on the drive before reporting the incident to the Connecticut attorney general and Insurance Department. Connecticut Attorney General Richard Blumenthal told the Hartford Courant, "The severity and scope of this breach is unprecedented in Connecticut, if not the country."

University of California San Diego's Moores Cancer Center Hit by a Hacker
On July 9, 2009, the University of California San Diego's (UCSD) Moores Cancer Center sent a letter to 30,000 patients, after a hacker breached its computers and gained access to patients' personal information. The computer servers were compromised on June 26 and contained information including patients' names, dates of birth, medical record numbers, and diagnosis and treatment dates back to 2004. The majority of the patients' information did not include Social Security numbers. Ms. DeAnn Marshall, UCSD Health Sciences' chief of marketing and communications officer stated that there is no evidence that any of the information has actually been viewed or used. Patients' medical records, which are stored in separate servers, were not breached, according to the cancer center. Authorities have been notified and an investigation is under way.

Federal Trade Commission Settles Latest Charges Against ChoicePoint
ChoicePoint, one of the largest data brokers, agreed to strengthen security to settle FTC charges that it failed to implement a comprehensive information security program protecting consumers' information, required by a previous court order. This failure left the door open to a data breach that compromised the personal information of 13,750 people and put them at risk of ID theft.

According to the FTC, in April 2008, ChoicePoint turned off a key electronic security tool used to monitor access to one of its databases, and for four months failed to detect that the security tool was off. During that time, an unknown person conducted unauthorized searches of the company's database containing sensitive consumer information, which included Social Security numbers. The searches continued for 30 days. Once the breach was discovered, ChoicePoint informed the FTC of the issue. ChoicePoint has agreed to expand its data security assessment and reporting duties and is required to pay $275,000.

Annual Study Reveals Data Breach Costs Keep Climbing
Data breaches cost healthcare organizations $282 per exposed record in 2008, according to a study released by the Ponemon Institute, a research organization devoted to privacy and data protection policy. The study, which examined the repercussions felt by companies that suffered breaches last year, also revealed that lost business made up nearly 70% of data breach costs. Healthcare organizations were the most susceptible to customer attrition following a data loss incident, experiencing churn rates — defined as the rate by which customers cease doing business with the breached firm — of 6.5%.

Related Links
- Fired Employees @ The Houston Chronicle: http://www.chron.com/disp/story.mpl/hotstories/6738856.html
- Information Breach @ Hartford Courant: http://www.courant.com/business/ht-healthnet1120.artnov20,0,1908752.story
- ChoicePoint @ DataBreaches.net: http://www.databreaches.net/?p=7870
- Data Breach Cost @ Bank Info Security: http://www.bankinfosecurity.com/articles.php?art_id=1188