

ISSUES FOR CONSIDERATION

- Often state laws have specific requirements regarding medical records and notification in the event of a breach. Please check with your state for details. AMA provides a listing of all state medical associations at <http://www.ama-assn.org/ama/pub/about-ama/our-people/the-federation-medicine/state-medical-society-websites.page>.
- The Practice should consider the potential breaches of employee information, i.e. social security number, banking information, address, etc. and should notify employees and offer identity theft protection. If the Practice has a method to contact individual employees, the media notification is not necessary.
- The Practice should be aware of Business Associates (BA's) and steps that are necessary for notification of breached information that falls under the BA's scope of work with the practice. BA's are required, under HITECH, to notify the Practice of the breach, including all of the information that is required under the Breach Notification rules.
- Notification can be put on a Practice website or done through a major print or broadcast media. We would recommend both to make sure that individuals have sufficient opportunity to access the breach information.
- Practices should always consult an attorney for legal guidance. These are guidelines to follow but should not be taken as legal advice.

Media Announcement

Practice Name – Notifies patients of a breach of unsecured protected health information (ELECTRONIC AND PAPER)

In accordance with the Health Information Technology for Economic and Clinical Health Act (HITECH) provision of the American Recovery and Reinvestment Act of 2009, **Practice Name** is required to notify you that we have experienced a breach of unsecured protected health information caused by the tornado that struck Joplin, Missouri on May 23, 2011.

The protected information that has the potential to be accessed includes patient financial and clinical information related to services through the Practice (i.e. Full Name, Social Security Number, Birthdate, Photos, Medical records number, etc., – this should include any identifiable information as described under HIPAA).

If you have reason to believe that your information was included in this breach you should contact any one of the nationwide consumer reporting companies to place a fraud alert on your credit report. The company you call is required to call the other two, which will also place an alert on their versions of the report. Contact information for each of these companies is included:

- Equifax 800-525-6285; www.equifax.com
- Experian 888-Experian (397-3742); www.experian.com
- Transunion 800-680-7249; www.transunion.com

In order to mitigate unauthorized use of the information accessed, acquired or disclosed, we have documented the data breach, evaluated our policies and procedures, and notified other parties associated with our practice, such as our Business Associates, as applicable. We have notified government entities and may also contact law enforcement, if appropriate.

We have established a toll-free number to call us with questions and concerns about the loss of your personal information. You may call (800) XXX-XXXX during normal business hours for additional information.

We also have a section on our Web site with updated information and links to Web sites that offer information on what to do if your personal information has been compromised.

We sincerely apologize for any inconvenience this may cause you and will help in any way that we can.

Signed

Practice Name