

March 31, 2009

# Health Information Security and Privacy Collaboration

## Privacy and Your Health Information: Tips to Protect Your Privacy

Prepared for

**RTI International**

230 W Monroe, Suite 2100  
Chicago, IL 60606

**Jodi Daniel, JD, MPH, Director**

**Steven Posnack, MHS, MS, Policy Analyst**

**Office of Policy and Research**

**Office of the National Coordinator for Health IT**

200 Independence Avenue, SW, Suite 729D  
Washington, DC 20201

Prepared by

Consumer Education and Engagement Collaborative  
Colorado, Washington, New York, Kansas, Massachusetts, Georgia, West Virginia

Health Information Security & Privacy

**COLLABORATION**



Contract Number HHSP 233-200804100EC  
RTI Project Number 0211557.000.007.100

Contract Number HHSP 233-200804100EC  
RTI Project Number 0211557.000.007.100

**March 31, 2009**

# **Health Information Security and Privacy Collaboration**

## **Privacy and Your Health Information: Tips to Protect Your Privacy**

Prepared for

**RTI International**

230 W Monroe, Suite 2100  
Chicago, IL 60606

**Jodi Daniel, JD, MPH, Director**

**Steven Posnack, MHS, MS, Policy Analyst**

**Office of Policy and Research**

**Office of the National Coordinator for Health IT**

200 Independence Avenue, SW, Suite 729D  
Washington, DC 20201

Prepared by

**Common Project Lead**

Dawn Bonder, Oregon

**Collaborative Members**

Phyllis Albritton, Colorado

Peggy Evans, Washington

Victoria Wangia, Kansas

Ellen Flink, New York

Jerilyn Heinold, Massachusetts

Alicia McCord-Estes, Georgia

Patricia Ruddick, West Virginia

Identifiable information in this report or presentation is protected by federal law, section 924(c) of the Public Health Service Act, 42 USC. § 299c-3(c). Any confidential identifiable information in this report or presentation that is knowingly disclosed is disclosed solely for the purpose for which it was provided.

## PRIVACY AND YOUR HEALTH INFORMATION:

### TIPS TO PROTECT YOUR PRIVACY

#### The Privacy of Your Health Information Is Protected By Federal Law

Most of us believe that our medical and other health information is private and should be protected, and we want to know who has or can see this information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, a federal law, gives you rights to your health information and sets rules and limits on who can look at and receive your health information.

#### Who Must Follow This Law?

We call the providers, businesses, and organizations that must follow the HIPAA Privacy Rule ***covered entities***.

Covered entities include:

- **Health plans**, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.
- **Most health care providers**—those that conduct certain business electronically, such as electronically billing your health insurance—including most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.
- **Health care clearinghouses**—entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Covered entities routinely establish relationships, typically through contracts, with other businesses to help them with particular programs or services. These businesses are commonly referred to as a covered entity's ***business associate***.

- **Business associates**—those businesses or organizations doing business with a covered entity must also follow the HIPAA Privacy Rule.

#### What Information Is Protected?

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

## How Is This Information Protected?

- Covered entities must have appropriate physical, technical, and administrative safeguards in place to protect your information.
- Covered entities must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose.
- Covered entities must have procedures in place to limit who can view and access your health information as well as implement training programs for employees about how to protect your health information.

## What Rights Does This Law Give Me Over My Health Information?

Health insurers and providers who are covered entities must comply with your right to:

- Ask to see and/or get a copy of your health records (you may be charged a reasonable fee for the copying of your record).
- 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 for marketing.
- Get a report on when and why your health information was shared for certain purposes.

## What Should I Do If My Rights Are Denied or I Don't Believe My Health Information Is Being Protected Properly?

- Contact a privacy officer.

Every health care provider and health plan covered by the federal health privacy law must appoint someone on their staff as a privacy officer. If you experience a problem related to the privacy of your medical records or access to them, you might want to contact this individual in an effort to resolve the problem.

- File a federal complaint.

You may also choose to file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights, the federal agency charged with enforcing the federal health privacy law. This office has the authority to impose civil and criminal penalties if they find a violation of the law. Your complaint must be filed within 180 days of the incident. You can also go directly to <http://www.hhs.gov/ocr/privacy/index.html>

- Seek state-level recourse.

There are officials in your state who may be willing to help you address violations of the federal privacy law and additional state privacy laws. Among those likely to help are your state attorney general <http://www.naag.org/>, your state insurance commissioner <http://www.naic.org/>, and a state medical board <http://www.fsmb.org/>. See the websites to find your state's officials.

- Explore lawsuits.

You do NOT have the right to sue a health care provider or health plan for a violation of the federal privacy law, but a documented violation of the federal law may strengthen a privacy case you bring in state court.

### **Who Can Look at and Receive Your Health Information?**

The law sets rules and limits on who can look at and receive your health information.

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

- for your treatment and care coordination;
- to pay doctors and hospitals for your health care and to help run their businesses;
- with your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object;
- to make sure doctors give good care and nursing homes are clean and safe;
- to protect the public's health, such as reporting when the flu is in your area; and
- 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 doctor or another covered entity generally cannot:

- give your information to your employer,
- use or share your information for marketing or advertising purposes,
- share private notes about your health care; and/or
- share your information with your health plan if you pay for the medical care in full and request that the information not be shared.

### **Employers and Health Information in the Workplace**

The HIPAA Privacy Rule controls how a health plan or covered health care provider discloses protected health information to an employer, including your manager or supervisor.

### **Employment Records**

The HIPAA Privacy Rule does not protect your employment records, even if the information in those records is health-related. Generally, the HIPAA Privacy Rule also does not apply to the actions of an employer, including the actions of a manager in your workplace.

If you work for a health plan or covered health care provider:

- The HIPAA Privacy Rule does not apply to your employment records.
- The HIPAA Privacy Rule *does* protect your medical or health plan records if you are a patient of the provider or a member of the health plan.

### **Requests From Your Employer**

The HIPAA Privacy Rule does not prevent your supervisor, human resources worker, or others from asking you for a doctor's note or other information about your health if your employer needs the information to administer sick leave, workers' compensation, wellness programs, or health insurance.

- However, if your employer asks your health care provider directly for information about you, your provider cannot disclose the information in response without your authorization.
- Covered health care providers must have your authorization to disclose this information to your employer, unless other laws require them to disclose it.

Generally, the HIPAA Privacy Rule applies to disclosures made by your health care provider, not to the questions of your employer.

### **What Can I Do to Protect My Health Information?**

- You should get to know the important rights listed above.
- You should ask your provider or health insurer questions about your rights.
- You should NEVER give health information to someone if you are not certain the person is authorized to have your information.
- You should not enter information online unless it is a secure website that you trust.
- You should not send e-mails that contain health information from a work e-mail address.
- You should not use a work computer to enter health information online.
- You should NEVER give health information to spammers (unsolicited e-mails).
- You should be conscious of your home computer security.

**Remember that YOU decide what information about yourself to reveal and when, why, and to whom.**