

March 31, 2009

# Health Information Security and Privacy Collaboration

## Frequently Asked Questions (FAQs): Privacy, Security, and Sensitive Health Information

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:  
Massachusetts

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**

## **Frequently Asked Questions (FAQs): Privacy, Security, and Sensitive Health Information**

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

Jerilyn W. Heinold, Massachusetts  
Diane L. Stone, Massachusetts

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.

## **BACKGROUND AND DESCRIPTION OF MA HISPC FREQUENTLY ASKED QUESTIONS (FAQS) PROJECT**

Massachusetts state law allows personal health information to be shared for treatment and payment purposes in most circumstances without a patient's consent. As a result, most kinds of health information can be routinely shared with other health care providers for treatment/consultation purposes, as well as payers for billing purposes. However, there are some situations when health information may not be disclosed to third parties without a patient's express consent. In most of those cases, such consent must be in writing. This requirement is because of Massachusetts' privacy statute, laws governing health care providers and insurers, and case law resulting from court decisions.

Certain kinds of "sensitive" information, including behavioral health information, genetic test results, and HIV test results, are subject to additional legal protections in Massachusetts. These additional protections may include a requirement that express written consent be obtained for each release of sensitive information, and other requirements relating to the form of the consent or other information that must be provided to the patient at the time of consent.

The risks and benefits of sharing information as well as questions regarding the viewing of information have not been well understood by consumers. Questions, for example, regarding health plan and employer viewing of sensitive information are consistently asked and are a source of concern for consumers. Breaches and remedies under federal and state law are also not well understood.

The HISPC Consumer Education & Engagement Collaborative has state initiatives that form one prong of a two-pronged approach to consumer education, the other being a set of projects that all member states participate in. This Massachusetts Frequently Asked Questions (FAQ) document is part of the Massachusetts five-project multimodal approach to educating and engaging consumers regarding the privacy and security of sensitive health information and its sharing requirements. It presents information in a "question and answer" format that is categorized by content. The content areas include risks/benefits, definitions, information sharing, patient rights, and security issues.

The 25 questions below were derived and ranked by the MA HISPC Workgroup (composed of behavioral health providers and consumer advocacy groups) because they were thought to be often asked or because there was uncertainty about the level of knowledge and/or misconception among consumers and providers in Massachusetts. The answers are written in a "direct to consumer" format using simple language and examples. The answers underwent legal review and review by the HISPC Consumer Education & Engagement

---

Collaborative, the MA HISPC Workgroup, and the MA HISPC Steering Committee; the answers were refined to reflect recommendations from each group.

---

## PROJECT 2—FREQUENTLY ASKED QUESTIONS AND ANSWERS FOR BEHAVIORAL HEALTH CONSUMER ISSUES

You may have questions about the privacy and security of your personal information in your medical records. Below is a listing of common questions. If your question is not included, you can ask your doctor or health care provider and he or she can help answer it.

### **Risk/Benefits**

1. What are the risks and the benefits if I consent to having my sensitive information shared electronically with other providers for treatment? In other words, what *can go wrong* and what *can be better* when I allow my sensitive information to be shared?

*Answer:*

### **BENEFITS**

Behavioral health information includes diagnoses, medications, and problems told to a health care provider. The benefits of consenting are greater compared with withholding this piece of information from providers. Sometimes a patient with behavioral health issues seems to have different medical symptoms from what a provider would expect for a medical condition. In this case, the provider may treat the patient for the wrong condition. The benefits of making behavioral health information available to providers for treatment are

- better patient care, because a provider has a full picture of key aspects of your condition;
- better quality and safety of care, when a provider does not have to guess about medications, diagnoses, or allergies;
- critical time saved in the emergency room; and
- less likelihood of unnecessary tests or duplication of tests.

### **RISKS**

The risk to you and your family when sensitive behavioral health information is shared is that it can get into the wrong hands. Behavioral health information (or any health information) transmitted electronically has the potential to get into a greater number of wrong hands than a paper file being shared inappropriately or incorrectly. Getting into the wrong hands is called a “breach” and can be unintentional or intentional.

## HELPFUL DEFINITIONS

### **Privacy Breach**

- Unintentional human mistakes can happen when someone who does not need or want to know your health information finds it in their hands or in front of their eyes. While this situation does not occur “on purpose,” your privacy has been breached. Even though this is a risk, you still need to balance your need for privacy of your

---

behavioral health information with the danger of it not being available to a provider when you need treatment.

- Your behavioral health information may be included as part of a provider's transmission to another provider, because it is part of your medical record. Again, this is a risk you need to consider as part of a balanced decision. If it is another provider who has received this additional information, the impact is typically minimal or nonexistent.
- In situations that are not provider to provider, you would have to authorize the provider who has your health information with a signed permission to release to another type of entity, for example, a life insurance company. It would not be a mistake in this case for the life insurance company to receive all of your medical information, because you signed an authorization to release it all. Yes, there is a possibility that you could be denied coverage or be quoted a higher premium when the behavioral health information is read.
- An intentional privacy breach could occur, for example, in child custody battles, when the noncustodial parent wants to prove the custodial parent is not competent. In this case, the noncustodial parent finds a way to obtain a copy of the custodial parent's history of medications or mental health visits. This action would be considered fraud on the part of the noncustodial parent, because he or she probably tricked the provider into releasing your health information.

## **Security Breach**

- An intentional security breach occurs when an Internet data thief gets into provider files (sometimes called "hacking") or steals a laptop computer. The result is that patient data are obtained for financial gain by selling to marketing companies, or research companies. In addition, there can be medical identity theft where care can be obtained using another's insurance coverage information. In this situation, the hacker would not have been after your behavioral health information necessarily, but the stolen files have included your information, causing you inconvenience and risk of potential personal discrimination.
- An unintentional security breach example occurs when a provider's office staff worker brings home medical files on a thumb drive or CD and loses the file.

The privacy and security industry has developed and continues to develop many techniques and computer programs to monitor and detect privacy and security breaches and prevent their occurrence.

---

## SHARING BEYOND PROVIDERS FOR TREATMENT PURPOSES

2. Can my employer see my sensitive information?

*Answer:*

Your provider is not permitted to disclose your sensitive behavioral health information to an employer without your written consent and authorization.

Some large employers “self-insure” medical benefits, and provide the medical coverage for employees directly. In these situations, the employer will have contracted with a health plan to just provide administrative services. These types of self-insured employers are allowed to have specific personnel, usually in a human resources department, have access to your claims information. These people are also legally bound to **not** disclose any health information about you to the rest of the company. Self-insured employers are bound by federal privacy and security laws.

3. What happens if my primary care physician prescribes medication for me that may indicate I have a condition that falls under the legal definition of sensitive, and then this doctor discloses my health record to a life insurance company when I apply for coverage?

*Answer:*

Remember, you would have to sign a consent or permission form authorizing your provider to release all data to a life insurance company. The result may be that you pay more for the insurance because you would be in a higher risk group or you may have more difficulty obtaining life insurance.

4. Does my health plan/insurer “have” my sensitive information? If yes, how do they protect my privacy? Are Medicaid claims handled differently?

*Answer:*

Yes, your health plan/insurance company will have information about sensitive health conditions if you have used your insurance to pay for services relating to these conditions.

If your insurer has received your provider’s claims for payment, these claims have to include enough information for the health plan to know it is an accurate, valid claim and is a covered benefit. To do this, the health plan needs specific information about the provider visit, a procedure code, a diagnosis, and a provider name and identification (ID) number.

Health plans are legally bound to protect the privacy of your behavioral health information under the same federal and state laws and requirements as your providers. Health plans are responsible to process and store claims on your behalf, and to maintain their records in their database.

Health plans also can use health information to develop health care trend information; this type of analysis is not intended to identify you as the patient. Statistical techniques are applied to the data to remove identifiers. This type of process is called “deidentification” or also may be called a “limited dataset.”

---

In general, your written authorization is required for a health plan to release your behavioral health information for most other reasons.

MassHealth is the Medicaid program in Massachusetts. Privacy and security rules for disclosure of patient information may be even stricter for MassHealth than for other health plan/insurance companies, because MassHealth must also comply with the federal Privacy Act and the state Fair Information Practices Act. In general, MassHealth will not release information about its members unless the information is part of providing benefits to the member (for example, to confirm member eligibility for benefits), or the member has provided permission for the release.

5. Are my child's health records in educational files at school protected if they contain diagnosis or treatment plans or medication information that is sensitive? What if the records are in the school nurse's files?

*Answer:*

Once a child's health records are put into a public school's records (elementary, secondary or post secondary school), they are no longer considered health records and not subject to Health Insurance Portability and Accountability Act (HIPAA) privacy rules. They are considered "educational records" and are protected by FERPA (Family Educational Rights and Privacy Act). FERPA applies to educational agencies and institutions that receive money from any program by the U.S. Department of Education. This includes most public schools and school districts.

At the elementary and high school level, a student's health record including immunization records, and medical records maintained by a school nurse, employed by or under contract with a school, are "educational records" subject to FERPA, **not** HIPAA. For example, a mental health record, which would be considered confidential information in a mental health provider's office, would be different if maintained by the school and subject to FERPA.

FERPA **does** require a parent or eligible student (at least 18 years of age) to provide written consent to share the student's educational records, or personally identifiable information from education record to others.

There are situations when sharing educational records may occur without written permission. These exceptions include the following:

- if teachers and other school officials have legitimate educational interest,
- in a medical emergency, and
- if knowledge of the information is necessary to protect the health or safety of the student or other individuals.

Parents and eligible students do have the right to inspect and review the student's "education records" and to seek to have them amended in certain circumstances.

It is important to note that many families do not have confidence in FERPA's protections. Many schools do not generally educate their staff about privacy in the same way health care staff are educated. The exception to this is HIV testing, which cannot ever be shared unless the parent gives specific permission in writing.

- 
6. Can a child's sensitive information be seen by family members, the health insurance coverage policy holder, or parents?

*Answer:*

**Yes**, in general, if the child is under 18, parents or legal guardians are allowed to see a child's sensitive health information. However, there are exceptions that will prevent family members and the policy holder from access without a child's authorization: a court order has barred parents from such information, a child who is considered a mature minor or emancipated, or a child who pays for his or her own care or who gets free care with counseling services.

**No**, if the child is 18 or older, even if the child is a dependent on the policy holder's health coverage. The policy holder needs the authorization from the child 18 or older to have access to sensitive information.

## **Patient Rights**

7. What is sensitive information, legally?

*Answer:*

Legally, sensitive information is a subset of medical information that is by law subject to specific conditions related to its creation, its release, or both. Under Massachusetts laws, "sensitive health information" is generally understood to include HIV/AIDS test results, substance abuse treatment information (substance "use" information is not considered sensitive information), most kinds of mental health information (including records of psychologists, social workers, and other therapists), mammography test results, abortion for minors, sexual abuse counseling, and genetic test results. The transmission of this information generally requires a patient's specific consent before it may be transferred. In some cases, one consent may cover multiple disclosures. In the case of HIV and genetic test results, however, consent must be obtained each time it is being shared. Many of these laws were passed to encourage people to seek testing and treatment without fear of exposure or discrimination.

8. Can I ask my physician to keep behavioral health information out of my EHR?

*Answer:*

You can ask, but the answer may be "no"; your behavioral health information will be stored on the physician's EHR. More and more, providers understand that paper files are not as efficient and usable as electronic files for quality patient care. Patient records in an EHR provide the opportunity to prompt for tests, appointments, and other types of reminders.

9. Can I ask that he or she not add certain information to the electronic record?

*Answer:*

You certainly have every right to ask for information to not be entered, but the decision on what the provider needs to render appropriate and necessary care will determine your provider's answer.

- 
10. What if I think information about myself or my family, other than legally defined health information, is sensitive?

*Answer:*

Currently, your rights to privacy of sensitive information are defined by law. While you cannot add to the legal definition, you can ask your providers to work with you on protecting additional information. Again, providers need key health information about you from records, and without that health information your care may be less effective.

11. I already signed consent when I registered or checked in at my physician's office. What did I agree to, and did it apply to my sensitive information?

*Answer:*

This answer depends on what a provider office asked the patient to sign at registration. Typically, at registration, you sign a "consent to treat" you for the symptoms that you present during the provider visit. Also, you consent to allow the provider to share parts of your health information to your health plan/insurer to be paid for providing you with services. You probably did not specifically sign consent to disclose behavioral health sensitive information. Such consent would have been clearly indicated on a form that you were signing, and it would have stated HIV, genetics, substance abuse, etc. (This could be one form or separate forms.)

Additionally, you may have been provided with the provider office Notice of Privacy Practices, which is a federal HIPAA requirement that tells you under what circumstances the provider can and cannot disclose your health information without your authorization. This was not a consent form; you were just informed about office procedures.

12. Is it OK to ask my primary care physician (PCP) what information he or she is planning to share with a referral to a specialist?

*Answer:*

Yes, it is definitely OK to ask your PCP what information he or she is planning to share. More than likely, your PCP intends to be very careful about sharing your information, because providers realize that patients trust them to do the right thing to protect patient health information.

13. When I give consent to release my behavioral health sensitive information, what type of people or organizations would be receiving my information?

*Answer:*

If you give written consent or authorization for the release of behavioral health sensitive information, the written form you sign will specify to whom the information is being sent, the purpose of the release of information, and how long the authorization would be in effect. Your information is most often requested for treatment, payment, or health care operations purposes.

14. May I get my copies electronically and/or can I download my information?

*Answer:*

---

If your electronic health information is maintained on a computer system, you may be able to get an electronic copy. You need to ask about it at your physician's office to see what format they can produce. Sometimes, you may only be able to get a printed paper copy.

15. What if information on my record is inaccurate?

*Answer:*

If some or all behavioral health information on your record is inaccurate, you need to notify the provider of the error(s) in writing and ask your provider to amend the record to add the information you have clarified or corrected.

16. Can police see my sensitive health information?

*Answer:*

In most circumstances, a court order is required for the release of information relating to substance abuse treatment or mental health therapy to law enforcement personnel. Usually, a judge will not permit the review of this information without making a specific finding that the need for the information in court outweighs the patient's privacy rights.

17. Can I ask my physician for a copy of everything he or she has sent my behavioral health sensitive information to; can I ask a hospital? Where is it stored?

*Answer:*

Yes, patients may ask their physicians for an accounting and receive information on disclosures of information made for reasons other than for treatment, payment, and health care operations. Currently there is no requirement to track information released for payment, treatment, or operations—all of which may be released without being tracked. In addition, there is no requirement to supply audit logs; there may be in the future.

Yes, you can ask your mental health/behavioral health providers for an accounting, but remember you will have provided the provider with written consent for release of this information to specific other parties.

Yes, you can ask a hospital where you received inpatient or outpatient care for an accounting of your behavioral health sensitive information that it may have disclosed. However, most hospitals cannot separate out the behavioral sensitive information. Hospitals can only account for information in general. Typically, a list would be provided to the patient that would say that the hospital released, for example, name, admission dates, diagnoses, and medications to XYZ provider.

If an EHR system contains your medical records, the data are stored on data drives that can physically be within the provider location or at an off-site secure location that is bound by federal and state law privacy and security requirements.

18. Who is allowed to view a patient's electronic health information including psychotherapy notes?

*Answer:*

---

Authorized individuals are allowed to look at your health information for treatment, payment, and health care operation activities. The rules for electronic health records are no different from paper health records. You should receive a notice of privacy practices upon a first visit to a provider, admission to a hospital, or joining of a health plan. As specified by HIPAA, these notices describe how your protected health information is to be collected, used, and transmitted for the purposes of treatment, payment, and health care operations. Also under HIPAA, your data may be accessed by law enforcement or national security officials if they present some form of legal document such as a warrant, subpoena, or summons.

HIPAA provides additional protections to psychotherapy notes maintained by mental health providers. These notes may not be disclosed for any purpose unless you provide a written authorization to do so. In addition, states have enacted privacy laws that clearly state categories of health information that are “sensitive” requiring a secondary consent from you at each transfer of information. In Massachusetts, that would include disclosures of HIV or genetic test results. HIPAA keeps health care providers and health plans from sharing your identifiable health information to employers without your written authorization.

Electronic health care processes in the future may give you greater control over the consent process and who sees your data, which in turn can help your physicians better manage your care.

Efforts funded by the federal government, such as the Health Information Security and Privacy Collaboration (HISPC), are developing privacy and security solutions to improve health information technology adoption and electronic health information exchange.

19. What can I do if I think my rights to privacy have been abused? Whom do I tell?

*Answer:*

Every provider’s Notice of Privacy Practices provides the information on whom to contact with privacy and security concerns and problems.

If you believe that your right to privacy has been abused, you need first to bring this to the attention of your provider, preferably in writing. If it is the health plan that you believe has abused your rights to privacy, you can call their published member services number on your ID card, and they have a procedure for you to follow for privacy concerns, they will connect you with the privacy officer.

20. Can I take back my consent?

*Answer:*

Yes, you can revoke your authorization or consent, but it becomes effective from that day forward; you cannot go back and reclaim any released data.

21. Will my care be negatively affected if I take back my authorization or consent?

*Answer:*

Your care should not be negatively affected by taking back consent to share with other providers. However, your provider may advise you that such a request is not in

---

the best interests of your medical care. Often this conversation results in a compromise.

## Security Issues

22. If my credit card and bank information is safe on a secure Internet site is my sensitive information in my record safe on the Internet too?

*Answer:*

The financial industry has been dealing with electronic transactions and transmission for more than 20 years; still your credit card and bank information are not completely safe—only relatively so. All industries are refining the security of data transmission. Health information from providers and payers is usually transmitted in a secure fashion and is governed by state and federal security rules designed to protect information. However, nothing is 100% secure and there is always some risk.

E-mail exchange between patient and provider is actually a greater risk to health information breaches than EHRs, because most patients do not use a secure e-mail system to communicate with their providers.

Also, patients need to remember that the laws that apply to information uploaded to personal health record sites such as those run by Google or Microsoft are limited.

23. How will I know if my health information has been breached?

*Answer:*

Once the entity holding your sensitive information knows that there has been a problem or a breach they are obligated under Massachusetts Data Security Laws to notify you and the Attorney General of the situation. Unfortunately, they cannot protect you from problems you may encounter as a result of that breach.

24. If I am adversely affected by a privacy or security breach, what are my remedies for compensation?

*Answer:*

If the privacy breach causes specific harm, you can sue for recovery of the effects of this privacy breach in a civil lawsuit under state privacy law. Intentional violations of privacy, such as the sale of information as part of identity theft, or computer hacking, may be federal crimes under HIPAA and other laws, and may be prosecuted by federal authorities.

25. How is my behavioral health sensitive data protected if it is provided to another state? Is every state the same?

*Answer:*

Federal laws, such as the HIPAA privacy regulation and the federal substance abuse regulations, are the same across state lines. However, additional laws protecting behavioral health information and consent vary from state to state.