Ensuring Patient Privacy

Bob Johnson, MPP
Office of Health Information Technology (OHIT)
Minnesota Department of Health

Minnesota e-Health Summit
June 17, 2015
Privacy & Security Considerations

• Privacy and security a key part of planning for an EHR
• Understand HIPAA compliance and establish privacy and security policies and procedures for your practice
  – Conduct security risk assessments
  – Establish breach notification procedures
  – Ensure electronic data are encrypted
  – Train your workers
• Follow industry best practices to minimize risk
Privacy & Security Resources

• Minnesota Standard Consent Form to Release Health Information
  – Q & A: Standard Consent Form to Release Health Information

• Summary of Proactive Monitoring Procedures for Secure Individual Identifiable Health Information

• Security Risk Analysis Tip Sheet

• HIPAA, Minnesota’s Health Records Act, and Psychotherapy Notes
MN e-Health privacy & security tools

www.health.state.mn.us/e-health/privacy
Standard Consent Form to Release Health Information

Instructions for Minnesota Standard Consent Form to Release Health Information

Important: Please read all instructions and information before completing and signing the form. An incomplete form might not be accepted. Please follow the directions carefully. If you have any questions about the release of your health information or this form, please contact the organization you will list in section 5.

This standard form was developed by the Minnesota Department of Health as required by the Minnesota Health Records Act of 2007. Minnesota Statutes, section 144.292, subdivision 8. The form must be accepted by a Minnesota provider as a legally enforceable request under the Minnesota Health Records Act. If completed properly, this form must be accepted by the health care organization(s), specific health care facility(ies), or specific professional(s) identified in section 3.

A fee may be charged for the release of the health information.

The following are instructions for each section. Please type or print as clearly and completely as possible.

1. Indicate your full and complete name. If you have a suffix after your last name (e.g., Jr., Sr.), please provide it in the “last name” blank with your last name. If you used a previous name, please indicate that information. If you know your medical record or patient identification number, please indicate that number. All these items are used to identify your health information and to make certain that only your information is sent.

2. If there are questions about how this form was filled out, this section gives the organization that will provide the health information permission to speak to the person listed in this section.

Completing this section is optional.

3. In this section, state who is sending your health information. Please be as specific as possible. If you want to limit what is sent, you can name a specific facility, for example Main Street Clinic. Or name a specific professional, for example chiropractor John Jones. Please use the specific lines. Providing location information may help make your request more clear. Please print “All my health care providers” in this section if you want health information from all of your health care providers to be released.

4. Indicate where you would like the requested health information sent. It is best to provide a complete mailing address as not everyone will fax health information. A place has been provided to indicate a starting difficulty for providing the health information. Providing a date is optional.

5. Indicate what health information you want sent. If you want to send the health information that is sent to a particular date(s) or year(s), indicate that on the line provided. For your protection, it is recommended that you initial instead of check the requested categories of health information. This helps prevent errors from changing your form. EXAMPLE: All health information.

6. If you select all health information, this will include any information about you related to mental health evaluation and treatment, concerns about drug and/or alcohol use, HIV/AIDS testing and treatment, sexually transmitted diseases and genetic information, and

Minnesota Standard Consent Form to Release Health Information

PAGE 1 OF 2

1 Patient information
   First name: ___________________________ Middle name: ___________________________
   Last name: ___________________________
   Patient date of birth: ______/____/____ (Previous names)
   Home address: ________________________
   City: ________________________ State: __________ Zip code: __________
   Daytime phone: ________________________ E-mail address (optional): __________
   Medical Record/Patient ID number (optional): __________________________

2 Contact information about how this form was filled out (optional):
   First name: ___________________________ Last name: ___________________________
   Please indicate who the form was completed by (if this is someone other than you).
   Address: ___________________________
   City: ________________________ State: __________ Zip code: __________
   Phone (optional): ________________________ Fax (optional): __________
   Information needed by (date): ______/____/____ (optional)

3 I am requesting health information be released from at least one of the following:
   Organization(s) name: ________________________________________________________
   Specific health care facility or location(s): __________________________________________
   Specific health care professional’s name: __________________________________________

4 I am requesting that health information be sent to:
   Organization(s) name: ________________________________________________________
   And/or person: First name: ___________________________ Last name: ___________________________
   Mailing address: ________________________________________________________________
   City: ________________________ State: __________ Zip code: __________
   Phone (optional): ________________________ Fax (optional): __________
   Information needed by (date): ______/____/____ (optional)

5 Information to be released
   IMPORTANT: Indicate only the information that you are authorizing to be released.
   □ Specific dates of your treatment
   □ All health information (see description in instructions for what is included)
   □ OR only release specific portions of your health information. Indicate the categories to be released:
     □ History/Physical
     □ Mental health
     □ Discharge summary
     □ HIV/AIDS testing
     □ Laboratory report
     □ Radiology report
     □ Laboratory report
     □ Radiology report
     □ Emergency room report
     □ Photographs, videos, digital or other images
     □ Surgical report
     □ Other information or instructions:
     □ Medical Record
     □ Medical Record
     □ Other information or instructions:
     □ Immunizations

   The following information requires special consent by law. Even if you indicate all health information, you must specifically request the following information in order for it to be released:
   □ Chemical dependency program pre-admission and initial evaluation
   □ Psychotherapy notes (this consent cannot be combined with any other consent instruction)

This form was approved by the Commissioner of the Minnesota Department of Health on January 30, 2008 and updated in July 2014.
MN Model Notice of Privacy Practices

Your Information. Your Rights. Our Responsibilities.

OCTOBER 2014

1. Header

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

2. “Your Rights”

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

3. Copy of medical record

Receive an electronic or paper copy of your medical record

- You can ask to see or copy an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health information within a reasonable time.
- If you ask to see or receive a copy of your record for purposes of reviewing current medical care, we may not charge you a fee. [Minn. Stat. § 144.292 subd. 6]
- If you request copies of your patient records of past medical care, or for certain appeals, we may charge you specified fees. [Minn. Stat. § 144.292 subd. 6]

4. Request to amend medical record

Ask us to correct your medical record

- You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.
- We may say “no” to your request, but we’ll tell you why in writing within 60 days.

5. Request confidential communications

Request for us to contact you confidentially

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will say “yes” to all reasonable requests.
Summary of Proactive Monitoring Procedures

### Table 1: Summary of Proactive Monitoring Procedures

<table>
<thead>
<tr>
<th>PROCEDURE</th>
<th>HOW METHOD IS USED</th>
<th>EXAMPLES</th>
</tr>
</thead>
</table>
| Staff Education to promote a culture of awareness | Conducting Planned and Scheduled Education, Training and Communication                                                                                                                                             | 1. Use training events as a time to ask for staff feedback or questions related to health information safety  
2. Results and feedback can be used as a way to monitor perceived risks to the organization  
3. Sending compliance reminder emails routinely  
4. Annual Staff Training on Privacy Security Topics |
| Conducting privacy rounds and physical monitoring of building and activities | Compliance staff are visible and accessible in health care setting or organization                                                                                                                               | 1. Physical “Walk-Through” of facility to monitor staff  
2. Use an official audit tool to complete a walkthrough of an area  
3. Review physical safeguards including security of documents, verbal disclosures, proper disposal, white boards/bulletin boards, etc.  
4. Review technical safeguards: unattended computer monitors, use of computer lockouts, etc.  
5. Review staff knowledge and understanding of privacy-related matters (e.g., how do they manage PHI, how to report a privacy concern, ask questions, etc.)  
6. Ask staff what help they need to protect PHI better within their area  
7. Generate an official report with action plans to ensure accountability |
| Tracking and Trending                           | Baseline tracking and ongoing trend of incidents or unusual patterns of activity                                                                                                                                  | 1. Use results to build monitoring and auditing  
2. Identification of educational needs  
3. May lead to needed updates in policies, procedures, training, etc. |
| Monitoring Electronic Health Record access to records of “High Profile” Patients | Tracking access of EHR by staff and contractors when high profile patients or clients access medical care                                                                                                  | 1. Monitor Current Events:  
   - Scenarios in news/making persons vulnerable  
   - Using Google alerts  
   - Vulnerable populations  
   - VIP (e.g., public figures, celebrities, retired clergy, board members, highly visible employees/members of medical staff, etc.) |
| Performing Random Focused Audits of Electronic Health Record access | Manual random audits that are created based on case by case need                                                                                                                                                | 1. Medical emergency actions  
2. Work unit audit logs:  
   - Sorting by job titles  
   - Use of data analytics tools |
Security Risk Analysis Tip Sheet

What is a Risk Analysis?
The HIPAA Security Rule requires organizations that handle protected health information to regularly review the administrative, physical and technical safeguards they have in place to protect information. By conducting risk analysis, healthcare providers can uncover potential weaknesses in their security policies, processes and systems. Risk analysis also helps providers address vulnerabilities, potentially preventing health data breaches or other adverse security events while supporting improved security of patient health data.

A risk analysis is foundational to any compliance program and is built on guidance from NIST SP 800-30 Standards.

How it is completed will depend on the size, complexity and capabilities of the organization. Core Elements of a Risk Analysis are listed in Table 2.

Table 2: Core Elements of Risk Analysis

<table>
<thead>
<tr>
<th>CORE ELEMENTS OF RISK ANALYSIS</th>
<th>REQUIREMENTS</th>
<th>RESULTS AND OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope of the Analysis</td>
<td>The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization creates, receives, maintains, or transmits (45 C.F.R. § 164.306(a)).</td>
<td>This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media or portable electronic media.</td>
</tr>
<tr>
<td>Data Collection</td>
<td>An organization must identify where the e-PHI is stored, received, maintained or transmitted. (See 45 C.F.R. §§ 164.308(a)(1)(i)(A) and 164.310(b)(1)).</td>
<td>An organization must identify where the e-PHI is stored, received, maintained or transmitted.</td>
</tr>
<tr>
<td>Identify and Document Potential Threats and Vulnerabilities</td>
<td>Organizations must identify and document reasonably anticipated threats to e-PHI. (See 45 C.F.R. §§ 164.202(a)(2) and 164.310(b)(8)(ii)). Organizations must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.310(b)(1(ii)(A)).</td>
<td>Organizations identify threats that are unique to the circumstances of their environment (e.g., viruses, spam, theft, fire). Organizations identify vulnerabilities (e.g., anti-virus software not updated, internet not encrypted, lack of policies and procedures).</td>
</tr>
</tbody>
</table>

1 Available at https://www.hhs.gov/privacy/hipaastandardsoverview/securityguide800-30.pdf

Security Risk Analysis Tip Sheet

October 2014

Minnesota Department of Health, Office of Health Information Technology | www.health.state.mn.us/health | MDHhealth.state.mn.us
HIPAA, Minnesota’s Health Records Act, and Psychotherapy Notes

Background
Patient access to psychotherapy notes in Minnesota may cause confusion among providers because of the unique interaction of federal and state law where state law wins.

- Federal law (HIPAA Privacy Rule) allows a mental health professional to share psychotherapy notes, at the provider’s discretion, with patient consent. In recognition of the sensitivity of this information, HIPAA requires that this consent be captured on a form only documenting the consent to release psychotherapy notes.

- Minnesota law is more stringent than HIPAA with respect to the rights of individuals. In Minnesota, patients have the right to view or release all parts of their medical record and psychotherapy notes are part of that medical record that can be viewed or released. The added protection of the notes inclusion in the medical record is to assure greater access for patients to all of their protected health information.

What’s in a medical record?
Much of the confusion stems from the differences in definition of what constitutes a medical record. Even if psychotherapy notes are kept in a separate file, in Minnesota, they are considered to be part of the medical record. This is to assure that patients have full access to complete information about their health.

Though this difference in definition of what is included in medical record may cause some alarm, in practice, these notes are rarely accessed. Minnesota does allow for the use of clinical judgment in the release of all medical records, such that if the release could cause harm to the patient or others, they can be withheld from the patient’s view.

HIPAA standard
Psychotherapy notes are specifically excluded from a patient’s general right to access or inspect their own medical records under HIPAA’s Privacy Rule. If mental health professionals wish to disclose the psychotherapy notes, they are generally permitted to do so, but must receive the patient’s authorization.

Minnesota standard
Minnesota’s Health Records Act gives patients access to “complete and current information possessed by that provider concerning any diagnosis, treatment, and prognosis” and does not distinguish psychotherapy notes from other medical records.
Other Community Resources

• REACH: http://www.khareach.org/

• Office of the Nat’l Coordinator: http://www.healthit.gov

• SAMHSA: http://www.samhsa.gov/health-information-technology

• Your professional associations
MN e-Health guidance

• Guide 1: Addressing Barriers to EHR Adoption
• Guide 2: Recommended Standards
• Guide 3: e-Prescribing
• Guide 4: Effective Use of EHRs
• Guide 5: Health Information Exchange

http://www.health.state.mn.us/e-health/reports.html
Things you can do now

• MN e-Health Roadmaps for Behavioral Health
  – Sign up for updates: https://public.govdelivery.com/accounts/MNMDH/subscriber/topics
    (scroll down to Provider Resources and select MN e-Health Roadmaps)
  – Learn about MN accountable health reform efforts: www.mn.gov/sim
  – Work with your association on establishing a technology committee to build consensus requirements and specifications for your health setting
MN e-Health Initiative

• Participate in the MN e-Health Initiative
  http://www.health.state.mn.us/e-health/
  – Sign up for the Weekly Update
  – Participate in workgroups

• Bob Johnson, MDH Office of Health IT
  bob.b.johnson@state.mn.us, 651-201-4856