Guidelines for Best Practices in the Use of Electronic Health Records and Social Media

- The speaker has no conflict of interest to declare
- This program did not receive any commercial support

Mary Ann Gapinski, MSN, RN, NCSN
School Health Advisor
MDPH

Electronic Health Records

Serve Multiple Purposes:
1. Legal documentation required by law and regulatory bodies
2. Communication system for healthcare providers
3. Implementation of quality improvement initiatives
4. Utilization review
5. Research and education
6. Grant application data
7. Determining trends/ Surveillance (MDPH Reports)
8. Legal document in court proceedings
9. Reimbursement from third-party payers (i.e., Medicaid, Medicare)
10. Standardization of documentation

EHR Basics

Every student must have a School Health Record:
- Demographics
- Immunizations
- Licensed Provider Orders
- Individualized Healthcare Plan
- Sequential Narrative Notes
- Services and Treatments
- Outcomes of Procedures and Interventions

EHR Basics (continued)

- Accurate
- Standardized
- Cumulative
- Specific
- Objective
- Confidential
- Legal
- Transferable
EHR Basics (continued)
May Or may NOT contain paper files such as:
- MA School Health Record face sheet
- Licensed prescriber’s physical exam form
- Medication and treatment orders
- Parent consent forms
- Lab reports
- Other health related correspondence
- Personal notes
  May still need paper record.

EHR Functions
1. Legal documentation required by law and regulatory bodies:
   - Must demonstrate that legal standards of school nursing practice have been met; Never document:
     - Abnormal findings without documenting intervention
     - Intervention without documenting evaluation/response
     - Evaluation/response without stating how it was evaluated
   - Provide evidence of standard of care provided.

If you didn’t document it....

You didn’t do it!

EHR Functions
2. Communication system for healthcare providers:
   - Must reflect optimal patient care in accordance with appropriate standards of care

EHR Functions
3. Implementation of quality improvement initiatives
   - Monitor health status of students and staff to identify school-wide problems
   - Evaluate effectiveness, accessibility, and quality of individual student and school-wide health services

EHR Functions
4. Utilization review
   - Identify frequent visitors/complaints as well as “under-utilized” services in order to improve resource allocation
   - Track risk factors (e.g., weight, behavioral health issues)
   - Flag missing data (e.g., immunizations)
EHR Functions

5. Use for research and education to assist with policy development and evidence-based solutions to health problems

6. Grant application data
   - Demographic
   - Local Providers
   - Health issues and problems
   - Local and state needs assessments
   - Federal reporting requirements

7. Determining trends/Surveillance
   - MDPH Monthly Report
   - MDPH Annual Report
   - MDPH BMI Report

   □ Public Health begins with surveillance...

   □ Without surveillance, you learn nothing at all.

8. Legal document in court proceedings:
   - Complete, consistent prior to closing
   - Timed, dated in sequence
   - Overwrite protection, automated audit trails

   Good documentation is an essential component of risk management!

   “Unclear, ambiguous or incomplete records are the leading cause that liability claims are filed and decisions are in the plaintiff’s favor”

   Schwab and Gelfman (2001)
EHR Functions

9. Reimbursement from third-party payers (i.e., Medicaid, Medicare)
   - Should follow documentation guidelines of insurance provider for appropriate reimbursement

EHR Functions

10. Standardization of documentation:
   - Common language and menu selections
   - Templates for interventions
   - Automated mathematical calculations and charting (e.g., BMI)

Challenges to EHR

- Garbage in....
- Garbage out!

Challenges to EHR (continued)

- Protection from loss and/or destruction
- Easily misdirected if not secure
- Must be able to address/ describe the security measures taken by the school district to protect confidentiality
- Protection of both “on-screen” and stored information

Challenges to EHR (continued)

- Secure passwords
- Virus protection
- “Hacker” proof
- Password-protected screen-savers
- Unattended computers
- Over-write protection
- Multi-level access
- Cost

Unauthorized Access: Lack of systems to ensure privacy, security, and appropriate sharing of student health information. (Must have “locked file cabinet”)

- Governed by FERPA (not HIPAA): considered education records – conflict between health and education laws
### Implementing EHS
- Vendor selection: plan first or select first – must support needs
- Test drive is optimal
- Technical assistance provided
- Know server options and capabilities
- Privacy and security capabilities
- Conflicts between EHR and paper-based systems
- Availability of technical expertise within the district

### Implementing EHS (continued)
- Vendor's stability
- Cost/ resources needed to connect with district's software
- Clarify costs including hardware, software, training, maintenance, technical assistance, updates, human resources, customized reports, etc
- Consistency in data entry required; may result in poor data, duplication, medical errors
- Power systems in school systems – IT vs Administration
- Ability for expansion...only just beginning!

### Technology-related concerns include:
- Answering machines/ Voice mail
- Cellular phones
- Texting
- Email
- Fax
- PDAs and USBs
- iPads and other “notebook” computers

### A word about email and texting....
- Informed consent should be obtained; should include:
  - Security measures to prevent breaches of confidentiality and privacy
  - Expected response time
  - Storage and access (printed copies)
  - Permission to forward
- School policies should address the type of information that can be sent via email
- Password protection imperative
- Encryption should be available
- Precautions to prevent mis-directed email
- Can be intercepted and reconstructed
- Confidentiality statement should be written on all email involving any student-specific information

### A word about email....
For secure email: must be encrypted – process to garble message and then allow the recipient to unscramble upon accessing (generally password protected) often via another website.

### A word about faxes....
- Must be direct to school nurse’s office
- Must include a cover sheet
- Create policies for proper authorizations for use
- Keep information limited
- School policy should state if original, signed document must also be obtained
Social Media and Other Electronic Communications

- Increasing exponentially
- Growing numbers of social media outlets, platforms and applications
- Facebook, LinkedIn, YouTube, etc
- Blogs, Online chat rooms, Listserves
- School and/or district websites, professional and personal websites

A word of caution....

- Provide for networking opportunities
- Opportunities for reflective practice
- District policies apply...few state or federal laws govern these communications
- HIPAA/ FERPA regulations apply
- Professional standards of conduct under BORN enforced
- Use of employer versus personal computer

Common Myths and Misunderstandings concerning Social Media

- Communication is private and accessible only by the intended recipient.
- Deleted content is no longer accessible.
- Communication is harmless (and private or confidential) if accessed only by the intended recipient.
- Referring to patient (student) by nickname, diagnosis, etc and not by name is acceptable.
- Confusion about "need-to-know" disclosure.
- Ease of sharing information via social media (including email) makes it a more acceptable means of communication.

Social Media Guidelines for Nurses

To view this YouTube video from NCSBN go to the resource section of this program and click on Social Media Guidelines

Thank you

Questions?

mary.gapinski@state.ma.us

617-624-5427