Mandatory Electronic Prescribing

And Other Fun Items

MARCH 27, 2015

- All prescriptions must be sent electronically or pharmacy won't fill it
- Exceptions rare and limited in scope
- What is it:

  Something transmitted electronically – not a fax; not an e-mail; not something printed from a computer

What Is It?

- Created, recorded, transmitted or stored by electronic means
- Issued and validated with the prescriber's electronic signature
- Electronically encrypted to prevent unauthorized access, alteration or use of the prescription
- Transmitted electronically directly from the prescriber to a pharmacy or pharmacist

What Must It Contain?

- Same information as a written prescription:

PLUS

1) NPI Number

2) Electronic signature

3) Specify dispense as written, if a brand-name product is therapeutically required

Exceptions

- Prescription to be filled outside of NY State
- System is down – electrical failure, no Internet
- E-prescribing would create harmful delay
- Waiver from Commissioner of Health (rare)

Not an Exception

- I don't have a computer – get one
- I like paper prescriptions – pharmacy won't fill

Policy Goals

- Minimize medication errors
- Integrate prescription records with EHRs
- Reduce prescription theft and forgery
- Pure politics – New York # 1

Controlled Substances

- Covers **ALL PRESCRIPTIONS** – no exceptions for small quantities or type of drug
- Controlled substances have additional requirements for security though – much more complicated:

    1) System must be certified as meeting DEA security requirements – two methods:

    a) DEA approved certifying body (very few)

    b) independent audit by third party

More on Controlled Substances

2) DEA requires a dual authentication protocol to access the e-prescribing system:
    a) any combination of two of the following:
        i) password or challenge question (something you know)
        ii) separate hard token (key) (something you possess)
        iii) biometric input (fingerprint, retina scan, etc.) (something you are)

More on Controlled Substances

3) Must register system with New York State Department of Health's Bureau of Narcotic Enforcement (no need to register system with DEA – no need to register system with DOH if system cannot transmit controlled substance prescriptions) – every two years and if software is upgraded/changed – also need DOH HCS account to do

http://www.health.ny.gov/professionals/narcotic/electronic_prescribing/

4) Identity proofing required: you need this in order to obtain the dual authentication that allows you to sign prescriptions

Identity Proofing

- Identity proofing is critical to the security of electronic prescribing of controlled substances. The authentication credentials used to sign controlled substance prescriptions may be issued only to individuals whose identity has been confirmed.
- You will be required to apply to certain Federally approved credential service providers (CSPs) or certification authorities (CAs) to obtain their two-factor authentication credential or digital certificate.
- The CSP or CA will be required to conduct identity proofing that meets **National Institute of Standards and Technology Special Publication 800-63-1 Assurance Level 3**. Both in person and remote identity proofing will be acceptable.

More on Controlled Substances

5) Access controls: two person system

Once you have been identity proofed and have your dual authentication credential, then you need to pass through access controls to use the electronic prescribing system.

Access Controls

- **Any e-prescribing application that meets DEA's requirements will require the practice to set access controls so that only individuals legally authorized to sign controlled substance prescriptions are allowed to do so.**
- **The e-prescribing application will determine whether access control is set by name or by role. If the logical access controls are role-based, one or more roles will have to be limited to individuals authorized to prescribe controlled substances. This role may be labeled "DEA registrant" or "dentist".**
- **Setting access controls requires two people. One person must determine which individuals are authorized to sign controlled substance prescriptions and enter those names or assign those names to a role that is allowed to sign controlled substance prescriptions. A DEA registrant must then use the dual authentication credential to execute the access control list. The access control list will need to be updated when registrants join or leave a practice.**

Sending the Prescription

6) Must be transmitted to pharmacy via secure encrypted method – the intermediary who handles the e-prescribing application will take care of that aspect
7) Pharmacy has its own set of rules to comply with at their end
8) Must report security breaches

NYSDA to the Rescue!

- NYSDA endorsed e-prescribing system:

Allscripts and Henry Schein

Three options:

1) Stand-alone e-prescribing system
2) E-prescribing system with new practice management system
3) E-prescribing system integrated with existing practice management system

NYSDA as GPO

4) Will integrate with existing Dentrix, Easy Dental, Dentrix Enterprise, PerioVision, EndoVision, OMS Vision, and Dental Vision Enterprise systems
5) NYSDA serving as Group Purchasing Organization (GPO) on behalf of members to obtain discounted rates – necessary for compliance with federal law – but members make their own choices – NYSDA GPO royalties fully disclosed to members

More on Endorsed Service

6) Can get an e-prescribing system for just non-controlled substance prescribing or for both controlled and non-controlled substance prescribing
7) Working on integration with Prescription Monitoring Program Registry (PMPR) with NYS Department of Health

Encryption

- Encryption is already incorporated into e-prescribing system – mandatory

What about e-mail?

E-mail is not a HIPAA-compliant secure method of transmission unless encrypted

BUT:

E-mail

- HIPAA does allow using regular e-mail to communicate with patients if the patient wants that and you have explained the risks of unencrypted e-mail to the patient
- Not for any third parties – only for patients

What is encryption?

- It is a process that complies with Federal Information Processing Standard (FIPS)

How to Encrypt

- Encryption can take various forms that meet FIPS:

    a) https – hypertext transfer protocol secure

    b) VPN – virtual private network

    c) secure browser

    d) other less common apps

Consult a computer systems security expert!

I Have Windows XP!!

- Sorry to hear that, but ……..
- HIPAA Security Rule does not mandate any standards for computer operating systems
- However – a system that lacks security is likely to eventually fail HIPAA security standards

DO A HIPAA SECURITY RISK ASSESSMENT!!

HIPAA Security Risk Assessment

- HIPAA has multiple parts: Privacy Rule, Security Rule, Transactions and Code Set Rule, NPI Rule, Breach Notification Rule, Enforcement Rule
- Security capabilities of the operating system may be used to comply with technical safeguards standards and implementation specifications such as audit controls, unique user identification, integrity, person or entity authentication, or transmission security.
- Any known security vulnerabilities of an operating system should be considered in the covered entity's risk analysis (e.g., does an operating system include known vulnerabilities for which a security patch is unavailable, e.g., because the operating system is no longer supported by its manufacturer).

How to Do Risk Assessment

- Office for Civil Rights (OCR), which enforces HIPAA, has issued online Security Risk Assessment Tool
- HIPAA requires doing a risk assessment
- http://www.healthit.gov/providers-professionals/security-risk-assessment to download the assessment tool
- The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

NYSDA to the Rescue!

- NYSDA also issues a manual for HIPAA Security Rule compliance (ADA also issues materials on this)
- NYSDA also has a HIPAA Privacy Rule compliance manual (ADA has materials on this too)
- NPI and Transactions/Code Sets Rules handled by NYSDA Health Affairs Department

Breach Notification

- Newest rule – part of HITECH Act -- Health Information Technology for Economic and Clinical Health (grand name, no?)
- Revise business associate contracts (business associate is any entity that you supply patient information to in order to do whatever it does for your practice – excluding insurers and health care professionals you refer to/consult – it also excludes dental and other laboratories)

More on Breach Notification

- HITECH made HIPAA Privacy and Security Rules directly applicable to business associates
- Includes breach notification – but health care professional remains equally responsible for breach notification
- If patient information is compromised, duty to notify kicks in
- 500 or more patients – must immediately notify HHS (even media)

What Is a Breach?

- Breach means the acquisition, access, use or disclosure of patient information in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the PHI.
- Examples: hacked computer system, lost/stolen laptop, identity theft
- Information must be stored or transmitted in electronic form – not applicable to purely paper records

I Have to Go to the Media??

- YES, if more than 500 patients have their information compromised; media means multiple prominent media outlets serving the area where the breach occurred
- For penalties, government looks at types of personal patient identifiers and the likelihood of re-identification, the unauthorized person who used the patient information (PHI) or to whom the disclosure was made, whether the PHI was actually acquired or viewed, and the extent to which the risk to the PHI has been mitigated

More on Breach

- Burden is on health care provider to establish these factors
- GOOD NEWS – if information was “secured”, then you escape all this

What is “Secured”?

- PHI has been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services.

Encryption Again!

- PHI that is encrypted **and** password protected is minimum needed to be considered "secured"
- Password alone not enough
- If not secured, then notify patients where it is reasonably believed PHI has been, accessed, acquired, used, or disclosed within 60 days of discovery

Notification Continued

- Notify the HHS Secretary for 500 or more patients within 60 days; for fewer than 500 patients, within 60 days after the end of the calendar year
- automatic OCR investigation for breaches involving more than 500 patients
- OCR can also do random HIPAA audits under HITECH (state AG can also enforce)

Penalties

- Penalty is required for willful neglect of HITECH obligations, which can be evidenced by ignoring HIPAA requirements or policies, failing to take steps to implement procedures called for by HIPAA, neglecting to adequately train staff, and not acting reasonably when HIPAA violations occur

How Much?

- Penalties can range from $100 to $50,000 per violation (already several multimillion $ cases)
- There is a maximum penalty capped at $1.5 million for all violations of the same provision of HITECH (violations of different provisions of HITECH can each generate up to $1.5 million, so there is no absolute limit)
- Penalties tiered based on degree of culpability

Penalties Continued

- 4 Tiers: lower penalties for a violation the covered entity 1) did not know about or would not reasonably have known about; or 2) due to “reasonable cause”; higher penalties for “willful neglect” either 3) mitigated or 4) unmitigated

OCR HIPAA Audit

OCR Audit can cover all the following:

- HIPAA Privacy Rule requirements for notice of privacy practices
- Rights to request privacy protection for PHI
- Access of individuals to PHI
- HIPAA administrative requirements
- Uses and disclosures of PHI
- Amendment of PHI
- Accounting of disclosures
- HIPAA Security Rule requirements for administrative, physical and technical safeguards
- The HITECH Breach Notification Rule requirements

NYSDA to the Rescue!

- Members have advantages in complying with the new electronic world
- NYSDA Technology Applications Task Force
- Regional Extension Centers (REC) of New York eHealth Collaborative (NYEC)
- http://nyehealth.org/
- Endorsed e-prescribing system
- More CE debuting at GNYDM