NATIONAL ASSOCIATION OF Community Health Centers

What You Need To Know About HIPAA Privacy

Presented By: Adam Bullian, JD
Director
QIP Solutions

Agenda

1. HIPAA Privacy Rule and PHI
2. Notice of Privacy Practices
3. Disclosures: Required, Permitted, and Authorized
4. Patients Right to Access, Amendment and Accounting;
5. Business Associates and Business Associate Agreements;
6. Essential Policies and Procedures.

HIPAA Privacy Rule

- One of three rules that make up HIPAA (privacy, security, and breach notification);
- Requires safeguards to protect the privacy of patient information;
- Sets limits on uses and disclosures of health information without patient consent;
- Specifies the patient's rights to their information, including accounting of disclosures, access to view and access to copies.
- Applies to Protected Health Information ("PHI"), whether electronic, paper, or oral form.

Protected Health Information

What is Protected Health Information?

It is personally identifiable health information (i.e. contains one of the 18 identifiers) that relates to,

- The individual's past, present, or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to the individual.

Essentially, it is any personally identifiable information related to the payment or delivery of health care.

PHI Identifiers

- Name
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Any vehicle serial number
- Device serial number
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual

Notice of Privacy Practices

- Describes the way in which you may use and disclose the patient's PHI;
- Must state your duty to protect privacy, provide a Notice of Privacy Practice, and abide by the terms of the Notice;
- Describes the patient's rights, including right to complain to you or Secretary of HHS if they think their rights have been violated;
- Must provide a POC for making a complaint or for more information.
- Must be,
  - Provided at time of first service (with an acknowledgement of receipt);
  - Posted in prominent location (i.e. waiting area); and
  - Posted on your website

Disclosures of PHI

Required Disclosures	• To the Individual • To HHS
Permitted	• Permitted, but not required • Patient consent not needed
Authorized	• Requires patient authorization • For disclosures not specifically permitted or required.

Required Disclosures of PHI

- Only two instances in which PHI must be disclosed,
  - To individuals when requested for access or an accounting of disclosures; and
  - To the HHS Secretary when conducting a compliance investigation, review, or enforcement action.

- All other other disclosures are either permitted or must be specifically authorized by the patient.

Permitted Disclosures of PHI

- Permitted disclosures may be made without the patient's consent, but they are not required to be made at all,
  - For treatment, payment, or operations;
  - With the potential to agree or object (i.e. facility directories, notifying family on individual's care, dispensing filled prescriptions to someone acting on behalf of the patient);
  - Incidental to otherwise permitted disclosure;
  - Public interest and benefit activities (i.e. public health activities, victims of abuse, health oversight activities, law enforcement, etc.); and
  - In a limited data set (direct identifiers have been removed).

Authorized Disclosures of PHI

- Any disclosure that is not required or permitted can only be made pursuant to a patient's authorization.

- Authorizations must,
  - Must in plain language;
  - Be specific about the information to be used/disclosed;
  - Identify the who is disclosing and receiving;
  - State a time or event for expiration; and
  - Permit the patient to revoke in writing.

- Can be for anything the patient wants,
  - Disclosure to an employer for pre-employment physical;
  - Disclosure to a pharmaceutical firm for marketing.

Patient's Right to Access

- Generally, patients have unfettered access to their own PHI.

- Limited exceptions to exist,
  - Psychotherapy notes; or
  - If could present a danger to the patient.

- They can review their PHI for **free** if requested.
  - Can request interpreter present during review.

- They can request a copy of their PHI in a form that is convenient for them (i.e. paper, e-mail) as long as it is not over burdensome for the provider.
  - Reasonable fees can be charged for copies and/or postage.

Patient's Right to Amend PHI

- Patients have a right to request a change to their PHI.

- Amendments do not have to be granted, but all amendments must be reviewed and processed.

- A process should be in place to,
  - Receive a requested amendment;
  - Review whether the amendment is warranted;
  - Communicate to the patient the outcome of the review;
  - If the amendment was granted, provide the amendment to whom the individuals request and anyone you know needs it.

Patient's Right to an Accounting

- Patient can request an accounting of disclosures: A list of who their PHI has been exchanged with and for what purpose. Includes transfers to Business Associates

- Must include transfers over the last 6 years.

- Do not need to include the following disclosures,
  - For treatment, payment, or operation;
  - To the individual or personal representative;
  - To those involved in individual's health care or payment;
  - Pursuant to an authorization;
  - Of a limited data set;
  - For national security or intelligence;
  - To correctional institutions; or
  - Incident to an otherwise permitted disclosure

Who Is A Business Associate?

Two Questions:

1. Does the organization in question perform a service or function on your behalf?

2. Do they need access to PHI to perform the service or function?

If the answer to both questions is ‘yes’, then they are your Business Associate.

Common FQHC Business Associates

- Electronic Health Record;
- Population Health Management Tool;
- IT Vendors/MSP;
- Payors that are neither government entities nor health plans;
- Consortiums/PCAs;
- Staffing Agencies;
- Cloud Storage Vendors;
- Etc…

Common Non-Business Associates

1. **Limited or Incidental Access to PHI:** Janitors, painters, and others who have incidental access to PHI, and/or spaces where PHI is stored, discussed, or viewed. Access to PHI is not required for them to perform the service or function.

2. **Conduits:** Those with a transient opportunity to view PHI or who access PHI on a random basis as necessary to transmit data. Examples include USPS, phone company, internet service provider.

What Is Required From Your BAs

1. A Business Associate Agreement must be in place will all of your Business Associates *before* they are provided access to PHI;

2. They must safeguard the PHI as outlined in the Business Associate Agreement;

3. May only access the minimum amount of PHI necessary for the purposes stated in the Business Associate;

4. Must notify you in the event they have a breach of PHI;

5. Although not specifically required, it may be appropriate to conduct a periodic review of your Business Associates compliance with HIPAA (i.e. request copies of recent incident investigations, most recent security risk assessment, and training log).

Business Associate Agreements

MUST INCLUDE:

1. Establish permitted uses and disclosures of the business associate;

2. State that the business associate will not use or disclose PHI for reasons not permitted or required;

3. Require business associate to implement HIPAA safeguards to prevent unauthorized use or disclosure;

4. Require business associate to report to CE unauthorized use or disclosure;

5. Require business associate to disclose PHI to satisfy CE's obligation to provide individuals with access to their PHI for amendments and accountings;

Business Associate Agreements

MUST INCLUDE:

6. Require business associate to comply with CE's privacy rule obligations as agreed;

7. Require business associate to make available to HHS information needed to show CE's compliance with HIPAA;

8. At the termination of the contract, require business associate to return or destroy the PHI;

9. Require business associate to ensure its subcontractors agree to the same provisions as the business associate agreed; and

10. Authorize the termination of the contract if business associate violated any material term (i.e. no's 1-9).

Policies and Procedures

- Provide the “how to” of keeping PHI private and secure in your organization.
- Ensures that safeguards are implemented consistently in times of staff turnover and crisis.
- Should be available to stakeholders to reference at all times.
- Should be periodically reviewed and updated.
- One person/role should be identified as the owner and should have responsibility for design, implementation, and review.

Policies and Procedures

Step-By-Step Guide:

1. Identify the policy owner and delegate;
2. Know the requirements for the specific issue and what is in place;
3. Determine the organization's position;
4. Draft the policy (templates can be very helpful, i.e. HIPAA COW);
5. Draft the procedure that will outline detailed implementation steps (including supporting documentation, i.e. logs, forms);
6. Distribute the drafts to stakeholders;
7. Approval of stakeholders;
8. Board of Directors approval; and
9. Schedule and calendar a time for review.

Essential Policies and Procedures

- Each organization should have certain policies and procedures, such as,
  - Password;
  - Privacy;
  - Acceptable Use
  - Minimum Necessary;
  - Training;
  - Incident Response;
  - Mobile Device/BYOD; and
  - Sanctions.

Additional Resources

1. Office For Civil Rights Privacy Rule Summary
2. Office For Civil Rights Guidance on Notice of Privacy Practices
3. Office For Civil Rights Sample Business Associate Agreement
4. HIPAA Collaborative of Wisconsin P&P Templates
5. Security and Privacy Blog

Questions and Next Webinar

Contact Information:
Adam Bullian
abullian@qipsolutions.com
(202) 594-5761

Next Webinar:
”How To Prevent A Cyber Attack At Your Health Center”
Friday, February 3, 2017
12:00 – 1:30 ET