Access Guidance and Enforcement Update

Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

Hyla Schreurs, J.D.
Supervisory Equal Opportunity Specialist

HIPAA Right of Access Guidance

- [http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html](http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html)
  - Comprehensive Fact Sheet
  - Series of FAQs
    - Scope
    - Form and Format and Manner of Access
    - Timeliness
    - Fees
    - Directing Copy to a Third Party, and Certain Other Topics
Access – Scope
• Designated record set broadly includes medical, payment, and other records used to make decisions about the individual
  – Doesn’t matter how old the PHI is, where it is kept, or where it originated
  – Includes clinical laboratory test reports and underlying information (including genomic information)

Access – Scope (cont.)
• Very limited exclusions and grounds for denial
  – E.g., psychotherapy notes, information compiled for litigation, records not used to make decisions about individuals (e.g., certain business records) BUT underlying information remains accessible
  – Covered entity may not require individual to provide rationale for request or deny based on rationale offered
  – No denial for failure to pay for health care services
  – Concerns that individual may not understand or be upset by the PHI not sufficient to deny access
Access – Requests for Access

- Covered entity may require written request
- Can be electronic
- Reasonable steps to verify identity
- **BUT** cannot create barrier to or unreasonably delay access
  - E.g., cannot require individual to make separate trip to office to request access

Access – Form and Format and Manner of Access

- Individual has right to copy in form and format requested if “readily producible”
  - If PHI maintained electronically, at least one type of electronic format must be accessible by individual
  - Depends on capabilities, **not** willingness
  - Includes requested mode of transmission/transfer of copy
    - Right to copy by e-mail (or mail), including unsecure e-mail if requested by individual (plus light warning about security risks)
    - Other modes if within capabilities of entity and mode would not present unacceptable security risks to PHI on entity’s systems
Access – Timeliness

Access must be provided within 30 days (one 30-day extension permitted) BUT expectation that entities can respond much sooner

Calculating Costs for Access Fees: 3 Acceptable Methods
1. Actual costs
   - Actual labor for copying (at reasonable rates, including only the time to create and send a copy in the form, format, and manner requested), postage, and supplies (paper, USB drive, toner, CD)
2. Average costs
   - Cost schedule based on average labor costs for standard requests is okay
   - Per page fee acceptable only for paper records (copied or scanned)
   - Applicable supply and postage costs may be added to average labor costs
3. Flat fee for electronic copies of electronic PHI only ($6.50 cap).
   - An alternative to calculating actual or average costs for certain requests
Access – Right to Direct PHI to 3rd Party

- Individual has right to have entity transmit PHI to 3rd party of individual’s choice (e.g., for research)
- Same requirements for providing access directly to the individual apply (e.g., fee limitations, form and format and timeliness requirements)

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY
Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach
- Business associate must notify covered entity of breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS of smaller breaches (affecting less than 500 individuals) permitted
- OCR posts breaches affecting 500+ individuals on OCR website

September 2009 through July 31, 2016

- Approximately 1,630 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 45% of large breaches
  - Hacking/IT now account for 12% of incidents
  - Laptops and other portable storage devices account for 29% of large breaches
  - Paper records are 23% of large breaches
  - Individuals affected are approximately 159,445,990
500+ Breaches by Type of Breach as of July 31, 2016

- Improper Disposal: 4%
- Loss: 9%
- Unauthorized Access/Disclosure: 24%
- Hacking/IT: 12%
- Unauthorized Access/Disclosure: 11%
- Other: 6%
- Improper Disposal: 4%
- Unknown: 1%

500+ Breaches by Location of Breach as of July 31, 2016

- Portable Electronic Device: 19%
- Laptop: 11%
- Network Server: 14%
- Desktop Computer: 11%
- Email: 8%
- EMR: 5%
- Other: 10%
- Desktop Computer: 11%
- Network Server: 14%
- Email: 8%
- EMR: 5%
- Other: 10%
What Happens When HHS/OCR Receives a Breach Report

• OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  — Public can search and sort posted breaches
• OCR opens investigations into breaches affecting 500+ individuals, and into a number of smaller breaches

General Enforcement Highlights

• Over 137,770 complaints received to date
• Approximately 885 compliance reviews initiated
• Over 24,331 cases resolved with corrective action and/or technical assistance
• Expect to receive 17,000 complaints this year

As of 3/31/2016
General Enforcement Highlights

• In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action

• In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action

• Resolution Agreements/Corrective Action Plans
  – 35 settlement agreements that include detailed corrective action plans and monetary settlement amounts

• 2 civil money penalties

As of July 31, 2016

Recurring Compliance Issues

Recurring Compliance Issues

• Business Associate Agreements
• Risk Analysis
• Failure to Manage Identified Risk, e.g. Encrypt
• Lack of Transmission Security
• Lack of Appropriate Auditing
• No Patching of Software
• Insider Threat
• Improper Disposal
• Insufficient Data Backup and Contingency Planning
Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- Implementing specific technical or other safeguards
- Mitigation
- CAPs may include monitoring

Some Good Practices:

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members’ critical role in protecting privacy and security
http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr

303-844-7508

Hyla.Schreurs@hhs.gov