HIPAA Access Guidance

Marissa Gordon-Nguyen
Office for Civil Rights
January 20, 2016

Components

- Fact Sheet
- Scope FAQs
- Form and Format and Manner of Access FAQs
- Timeliness FAQs
- Other (Clinical Labs) FAQs

FAQs in development

- Fees
- Directing access to a third party

General Right

- Access/copy upon request
  - By individual or personal representative
- Designated record set(s)
  - Group of records maintained by or for CE
  - Record = item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a CE

Examples of information subject to access

- Yes
  - EHR and/or paper medical record
  - Other medical, billing, payment, enrollment, claims records
  - Clinical laboratory test reports
  - X-rays, other images
  - Wellness and disease management program information
  - Clinical case notes
  - Old/archived PHI

- Access to DRS(s) held by BAs
  - CE ultimately responsible to provide access, regardless of where DRS maintained
  - BAA can specify that BA will fulfill requests (not just provide needed information to CE)
  - Request still must be fulfilled within time limits
- Clinical laboratories
  - DRS includes completed test reports, underlying data used to generate the reports, test orders, billing, insurance

General Right, continued

- Excluded information:
  - Quality assessment or improvement records
  - Patient safety activity records
  - Business planning
  - Provider performance evaluations
  - Psychotherapy notes
    - Maintained separately
  - Information for civil, criminal, or administrative action or proceeding

BUT

Included: Underlying PHI relied on in developing such records

Grounds for Denial of Access

- Unreviewable
  - Psychotherapy notes
  - Legal proceeding
  - Inmates (w/r/t copy)
  - DRS is part of research study still in progress, and individual agreed when consenting
  - Privacy Act protected records
  - Obtained under confidentiality
- Reviewable
  - Reasonably likely to endanger life or physical safety
  - Reasonably likely to cause substantial harm to a person referenced (not provider)
  - Access by personal representative reasonably likely to cause substantial harm

Details on denial of request for access

- Reviewable grounds
  - Reasonably likely to cause harm or endanger physical life or safety (very limited, rare)
  - Licensed health care professional exercises professional judgment
  - Ex. Suicidal patient
- Not grounds
  - Mere possibility of psychological or emotional harm

Denial of Access, continued

- Additional limitations
  - CE cannot require individual to provide a reason, or deny based on a reason offered or known
  - CE cannot deny access because BA maintains the PHI
  - CE cannot withhold or deny access because individual has not paid for health care services provided to the individual

Denial of Access, continued

- Carrying out denial
  - Provide denial in writing within 30 days of request (or 60 days if CE notified individual of extension)
  - Denial must be in plain language and describe basis, right to review and how to request (if applicable), and how to submit a complaint to OCR
  - If CE (or BA) does not maintain the PHI requests, but knows where it is, must inform individual
  - Must provide access to any other PHI requested
- Review of denial by professional not involved in original denial
  - Reviewing official must determine whether to reaffirm or reverse within reasonable period of time, and provide notice

Requests for Access

- Requiring a written request
  - CE may require requests in writing, including on CE's form
  - Must inform individuals of the requirement
  - CE may offer option of electronic request
  - Cannot create a barrier to or unreasonably delay access
- Verification
  - Reasonable steps to verify identity
  - Oral or written verification; authentication controls if electronic
  - Cannot create a barrier to or unreasonably delay access

Requests for Access, continued

- Unreasonable measures
  - Requiring individuals to go to office
  - Requiring individuals to use web portal
  - Requiring individuals to mail an access request

Providing Access

- Form and Format and Manner of Access
  - Provide in form and format requested if readily producible
  - Requests for paper copies
    - Provide paper copy
  - Requests for electronic copies
    - If PHI maintained only on paper, provide electronic copy if readily producible. If not, in readable hard copy or other form and format per agreement with individual.
    - If request PHI maintained electronically, must provide access in electronic form and format requested, if readily producible. If not, in agreed upon alternative electronic format. If individual refuses every offered electronic format, paper.

Right to an electronic copy

- Readily producible electronic copy of paper records
  - Ex. A scanned PDF version of PHI may be readily producible (but CE not required to purchase a scanner for this purpose), while a Word version of paper PHI may not be readily producible
- Right to receive information in human readable format
- Where CE is providing electronic copy, we also expect the copy to be in machine readable form to the extent possible, consistent with the request
- Right includes x-rays or other images in the record

Electronic Format Requested

- CEs not required to purchase new software or other equipment to accommodate every possible individual request
- Must have capability to provide some form of electronic copy if DRS is maintained electronically, which may require some investments (which cannot be charged to individuals)
- Whether format is readily producible depends on capabilities, not willingness
- Ex. Requested formats that may be readily producible
  - MS Word; MS Excel; PDF; structured, machine readable data; other electronic format
  - Particular technical standards such as RxNorm, LOINC

Access and Meaningful Use

- Under EHR Incentive Program, meaningful use includes providing patients the ability to View online, Download, Transmit health information
- VDT requirements are more exacting in some ways, but apply to narrower range of data (e.g., access is limited to information in Certified EHR Technology, but must be provided on a much shorter timeframe)
- If CE uses Certified EHR Technology, electronic PHI is readily producible
- CEs can use VDT mechanisms to fulfill access requests if individual requests or accepts the form/format/manner
- Individual always retains right to access PHI in a DRS that is not available through CEHRT
- See chart comparing HIPAA right to access and individual access opportunities under EHR Incentive Program

Providing Access, continued

- Form and Format and Manner
  - CE may provide summary of PHI requested (in lieu of access) or explanation of PHI (along with access), if individual:
    - Chooses to receive
    - Agrees to any applicable fees
  - Manner requested
    - Convenient time and place
    - Mail
    - Email (encrypted or unencrypted)

Readily producible method of copy/transfer/transmission

- Depends on capabilities and level of risk to security of PHI on the CE's systems, based on Security Rule risk analysis
  - Ex. Individual requests PHI downloaded to portable media provided by individual, but CE's risk analysis addresses potential use of external portable media and finds unacceptable level of risk. Individual may agree to purchase portable device from CE, or both agree on alternative form of electronic copy.
  - Ex. Individual requests that CE provide access by establishing direct connection between CE's system and individual's app or device. If capable and consistent with security measures, CE must provide access in this manner.

Unsecure transmission requested by individual

- We expect that CEs have capability to transmit PHI by e-mail, without unacceptable security risks to the CEs' systems
  - Limited exception may be where diagnostic image file sizes are too large to transmit via e-mail
- Thus, CE generally must agree to unsecure email transmission, but first must warn individual of the risk that PHI could be read or accessed while in transit
- 2015 edition CEHRT capable of sending unencrypted e-mail directly
- CE cannot require that individual accept unsecure method of transmission

Unsecure transmission requested by individual

- CE is not responsible for:
  - disclosures during unsecure transmission to the individual, provided warning given and risks accepted
  - breach notification obligations
  - safeguarding information once delivered to the individual
- CE is responsible for:
  - reasonable safeguards
  - in all other contexts, breach notification for unsecured transmissions, and may be liable for impermissible disclosures that occur in transit

Providing Access, continued

- Timeliness
  - No later than within 30 days from when request was received, either by the CE or its BA
  - If unable to meet 30 days, CE may extend to 60 days
    - Must notify individual within initial 30 days
    - Only one extension per access request

Timeliness

- Timeliness requirements apply to old, archived, or otherwise not readily accessible information
- Negotiating with individual on format of the response depletes the allotted time
- Outer limit. In many cases, CE may be able to provide quicker access
- Provide information in pieces as available, if individual wants

- EHR Incentive Program
  - Participating providers may use CEHRT engagement tools to make certain information available quickly and satisfy EHR Incentive Program objectives
  - Certified EHR Technology tools for access can speed up access
- Why not require faster access?
  - Still some circumstances in which additional time is needed to locate and obtain requested PHI
  - HHS will monitor developments, consider again whether to set higher expectations for responding to all requests

Clinical Laboratories

- If test will take more than 30 days to complete, lab may extend up to the maximum 60 days after notifying individual (within initial 30 days) of the reason for delay
- If test will not be complete within 60 days, individual has the right only to PHI in the DRS at the time the request is fulfilled
  - Ex. Test requisitions, underlying data used to generate reports, other completed test reports
- If lab knows test report will take longer than 60 days, the lab should inform the individual, who may withdraw or hold request until later to ensure full access

Clinical Laboratories

- Not required to interpret test results for patients
- May refer patients with questions about results to ordering or treating providers
- May provide educational or explanatory materials regarding the test results
- May include a disclaimer, caveat, or other statement explaining limitations of the laboratory data for diagnosis, treatment, or other purposes

Providing Access, continued

- Fees for copies
  - Reasonable, cost-based
    - Labor for copying PHI
    - Supplies for creating copy
    - Postage, if mailed
    - Preparation of explanation or summary, if individual agrees
  - Does not include*
    - Verification
    - Documentation
    - Search/retrieval
    - Maintaining systems
    - Recouping capital
    - Other costs

* Even if authorized by state law

Other

- Right to direct PHI to another person
  - Request must be in writing
  - Same requirements for providing access apply
- State laws
  - Some require access in shorter time frame; CEs responsible to comply
  - Contrary laws preempted by HIPAA unless exemption exists

Questions?

www.hhs.gov/hipaa