Medical Records Issues: Content, Maintenance and Retention

September 22, 2016

Teresa D. Locke

HOLLAND&HART

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

HOLLAND&HART

Overview

- Documentation and content of medical records
- CMS regulations and interpretive guidelines for medical records
- Making revisions, additions or corrections to medical records
- Retention, access and transfer of medical records
- Security and storage issues
- Additional resources

HOLLAND&HART

Helpful Written Materials

- .ppt slides
- http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/SE1022.pdf

Medical Records – Why This Matters

Medical Records – Why This Matters

- Proper medical records are critical to:
  - Patient care
    - quality of care
    - continuity of care
  - Legal compliance
  - Payment and reimbursement
  - Risk management/malpractice claims
  - Continued employment/retention of privileges
  - Liability insurance
  - Appropriate utilization review and quality of care evaluations

HOLLAND&HART

Medical Records – Potential Liabilities

- Civil lawsuits, fines and penalties
  - Malpractice
  - False Claims Act
  - Lack of informed consent
  - Violation of privacy
  - Spoliation of evidence
  - Exclusion of key evidence

Medical Records – Potential Liabilities

- Criminal penalties:
  - Fraudulent claims
  - Improper destruction of records pending investigation
  - Violation of HIPAA privacy
- Administrative sanctions:
  - Licensing actions
  - Exclusion from Medicare/Medicaid
  - Civil monetary penalties
  - NPDB report

Medical Records – Potential Liabilities

- Adverse business consequences:
  - reduced or denied payments
  - loss of hospital or facility privileges
  - loss of participation in third party payment program
  - loss of insurance coverage
  - loss of reputation

Medical Record – What is it?

HOLLAND&HART

Medical Record – What is it?

- "Medical record" is a subset of documents and data that you maintain relevant to a patient.
- What is/should be in the "medical record" depends on the context and reason for defining the record:
  - Provision of and payment for medical care.
  - Regulatory and statutory requirements.
  - Access by patients.
  - Responding to legal process (e.g., court order, warrant, subpoena, etc.)

Medical Record – Patient Care and Operations

- Generally include documents/data necessary to:
  - document patient's health and healthcare
  - provide a means for communication between practitioners caring for the patient
  - provide a basis for evaluating adequacy and appropriateness of care
  - support claims for payment or reimbursement
  - protect legal interests of patient and provider
  - provide clinical data for planning, research and education

Medical Records – Patient Access

- Per HIPAA, patient and personal representatives generally may access information the patient's "designated record set."
  - Includes right to inspect, obtain a copy or both.
- Must provide info whether maintained by a covered entity, or by a business associate on behalf of a covered entity, regardless of the date the information was created; whether the information is maintained in paper or electronic systems onsite, remotely, or is archived; or where the PHI originated (e.g., whether the covered entity, another provider, the patient, etc.)

Medical Records – Patient Access

- Must provide info in the form and format requested if readily producible in such form.
  - request for paper, must be paper
  - request for electronic copy of paper records, must scan and produce electronically if able
  - request for electronic of electronic records, must be electronic
- Must provide access in the manner requested.
  - cannot require that an individual to come to physical location to pick up a copy if she requests that the copy be mailed or e-mailed
- Must provide in a timely manner (no later than 30 days after receipt of the request).
- May impose reasonable, cost-based fee for labor, supplies and postage.

Medical Record v. Designated Record Set

- "Designated Record Set" is defined as:

A group of records maintained by or for a covered entity that are:

- The medical records and billing records about individuals maintained by or for a covered health care provider;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the covered entity to make decisions about individuals.

The term "record" means any "item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity."

45 CFR 164.501

Medical Records – Patient Access

- Covered entity can only deny access to designated record set on certain grounds – examples include:
  - psychotherapy notes
  - information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
  - PHI created/obtained in the course of research while research is in progress
  - PHI obtained under promise of confidentiality and access would reveal source of information
- If access denied on other basis, patient has right to have denial reviewed by a licensed health care professional designated by the covered entity.

45 CFR 164.524

Medical Records – Patient Access

- If covered entity denies the request:
  - Must give access to other info to the extent able.
  - Must provide written explanation, including:
    - Basis for denial.
    - Right to submit denial to independent review (if applicable)
    - Right to complain to covered entity, including the name, title and phone number to whom complaints are directed.
  - If the covered entity does not maintain the info, it must tell the patient where the info is located.

45 CFR 164.524

Medical Records – Patient Access (Representative)

- An individual also has a right to direct the covered entity to transmit the PHI about the individual directly to another person or entity designated by the individual.
- Must be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI.
- A covered entity may accept an electronic copy of a signed request (e.g., PDF), as well as an electronically executed request (e.g., via a secure web portal) that includes an electronic signature.
- The same requirements for providing the PHI to the individual apply.

45 CFR 164.524

HOLLAND&HART

Medical Records – Patient Access

- A covered entity must document the following and retain the documentation as required by 45 CFR 164.530(j):
  - The designated record sets that are subject to access by individuals; and
  - The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

45 CFR 164.524

Medical Records – Patient Access under State Laws

- State laws that provide individuals with greater rights of access to their PHI than the Privacy Rule, or that are not contrary to the Privacy Rule, are not preempted by HIPAA and thus still apply.
  - e.g., shorter time frame for production
- Unless an exemption exists in the HIPAA Rules, State laws that are contrary to the Privacy Rule access provisions – such as those that prohibit certain laboratories from disclosing test reports directly to an individual – are preempted by HIPAA. See 45 CFR 160.203. Thus, these State laws do not apply when an individual exercises her HIPAA right of access.

Medical Record – Other Practitioners

- HIPAA allows sharing of info with other practitioners for purposes of treatment, payment, and some health care operations.
  - No authorization required
  - Minimum necessary standard does not apply
- Generally not required to share info except:
  - Standard of care may require disclosure
  - If patient requests that records be sent to another provider
  - If Medicaid patient reassigned to another primary care physician, must send copies of records

45 CFR 164.506

Medical Record – Legal Process

- Generally no legal definition of "medical record."
- Ultimately, bound by terms of subpoena, order, warrant, or law regardless of internal definition.
  - If they ask for it, generally must provide it unless object or obtain waiver.
  - If they don't ask for it, generally not required to produce it.
- If request is broad (e.g., all medical records of the patient), must turn over all records regardless of who created it.
- May ask for clarification or limitations.
- May help to adopt policy defining the "medical record" to support your response but not failsafe solution.

Defining the Medical Record

- Each organization should establish its own medical record policies after considering—
  - Clinical needs (provide quality patient care)
  - Business needs (for payment, planning, etc.)
  - Legal needs (preserving evidence)
  - Statutes and regulations
    - state licensing regulations
    - Conditions of Participation
  - Accreditation standards
  - Third party payor requirements
  - Community standard of care
  - Practical concerns (e.g., space, time, duplication, etc.)

Defining the Medical Record

Generally includes…

- Advance directives
- Consents
- Intake and registration
- History and physical
- Allergies
- Immunization
- Records from other providers if relied on to provide care
- ED records
- Care plans
- Orders
- Medication administration
- Assessments
- Progress notes
- Images and photos
- Diagnostics
- Labs, radiology, test results
- Pathology
- Therapy
- Operative and procedure reports
- Consultations
- Provider-patient or provider-provider communications
- Discharge summaries
- Discharge instructions
- Etc.

Defining the Medical Record

- Generally does not include . . .
  - Psychotherapy notes
  - Administrative documents
  - Billing or payment
  - Protocols and pathways
  - Quality assurance
  - Peer review
  - Patient complaint or satisfaction forms
  - Compliance, including HIPAA
  - Requests for records
  - Public health reports
  - Statistical reports
  - Attorney-client communications
  - Etc.

HOLLAND&HART

Defining the Medical Record

- Don't forget to consider the non-traditional or "hidden" records . . .
  - Electronically-stored records or EHR
  - Email
  - Images
  - Data captured by machines
  - Data stored in different systems
    - e.g., labs, cardiology, PACS, etc.
  - Audio or video files
    - e.g., dictation, telephone consults, telemedicine, etc.

Defining the Medical Record

- COP: Clinical Records (42 CFR 485.638)
  - identification and social data
  - informed consent forms
  - pertinent medical history
  - assessment of health status and health care needs
  - summary of episode, disposition and instructions
  - reports of physical exams, diagnostic and lab results
  - consultative findings
  - all orders
  - reports of treatments and medications
  - nursing notes
  - documentation of complications
  - dated signatures of health care professionals

Defining the Medical Record

- Consider problem issues—
  - Records received from other providers, including those not relied on to provide care.
  - Personal health records (i.e., created or provided by patient)
  - Working notes, draft records, or other incomplete records.
  - Emails, text messages, web messaging, or other e-communications.
  - Duplicates.
  - Duplicates with additional notations.

Transitioning from Paper to EMR

- Must ensure that patient care and appropriate record-keeping practices continue without interruption.
- If converting paper to electronic format, must ensure integrity of the data.
- Establish specific procedures for converting files and document these procedures in writing.
- Quality assurance: verify that documents have been properly scanned.
- Ensure that entire record is intact, including all attached notes and handwritten comments.
- Consider retaining paper charts for a period.

Medical Records – What Should/Must They Contain?

HOLLAND&HART

Medical Records - Content

- Provider should maintain a record for every individual assessed or treated.
- May need to document contacts even if no "medical record" as result of assessment or treatment—
  - Patients who show up at ER.
  - Patients who call but do not show for appointments.
  - Patients who leave AMA.
  - Patient phone calls and emails.
  - Consultations.

Medical Records - Content

- Record should contain sufficient information to:
  - Identify the patient, including patient name and health record number on every page.
  - Support the diagnosis.
  - Justify the treatment.
  - Document the course and results of treatment.
  - Promote continuity of care among providers.

  (See 42 CFR 482.24)
- Additional regulations, standards, and contract terms may require further content.

Medical Records - Content

- Among other things, medical records should document:
  - Informed consent for treatment
  - History of present complaint and relevant past history
  - Examination/inventory of systems
  - Provisional diagnosis
  - Observations and progress notes, including changes in condition
  - Diagnostic test results
  - Orders
  - Patient status
  - Treatment
  - Significant events or incidents
  - Conclusions
  - Communications with patient and others

42 CFR 482.24(c)

HOLLAND&HART

Remember . . . .

- If it's not in the chart, it didn't happen.
- If the chart can't be found, it's because you're hiding something.
- Medical records often are the most important objective evidence physicians and hospitals can offer in their defense against malpractice claims.
- Aside from legal considerations, the most important reason for healthcare providers to maintain accurate, credible medical records is that good documentation protects patients.

Medical Records - Content

- Display drug allergy information in prominent and consistent location, e.g., brightly colored sticker on the cover of the chart.
  - Periodically update allergy information
  - Consider medication control record
- For patients with the same name (e.g., children of another patient), include some notice or warning.
- Place documentation in reverse chronological order (most recent on top) – be systematic.
- Separate portions of lengthy records with dividers
  - History and physical, patient visits, lab results, correspondence

Medical Records - Content

- Make sure all papers are attached to the file.
  - No “free floating” papers
  - No “post-it” notes
  - May staple such items to regular paper.
- Document—
  - Patient education/instructions (including on drugs)
  - Missed appointments/canceled appointments
  - Noncompliance
  - Return visit advice
  - Referral notes
  - Disruptive conduct

* May document patient complaints in separate file.

Medical Records - Content

- Document phone calls in chart – documenting in separate log is risky
  - develop procedure with office staff for phone calls
- Ensure that e-mails is in the record the same as an in-person encounter
- Consider a "problem list" in group practice charts.
  - identify serious medical conditions
  - alerts co-treaters to review progress notes and correlate treatment or follow-up advice
  - problems list must be current and complete, however, in order not to mislead
- Red flag medical problems that are not resolved for follow-up on next visit.

Medical Records - Entries

- Practice/provider should determine who may make entries.
  - Generally no law governing those who are authorized to make entries.
  - HIPAA requires that covered providers establish policies identifying those with access. (45 CFR 164.530)
  - CMS specifies that in order to meet the meaningful use objective for computerized provider order entry (CPOE), any licensed health care provider or a medical staff person who is a credentialed medical assistant or is credentialed to and performs the duties equivalent to a credentialed medical assistant can enter orders in the medical record, per state, local and professional guidelines. The remaining meaningful use objectives do not specify any requirement for who must enter information.

Medical Records - Entries

- Direct treatment providers should make entries in the medical record documenting their care.
  - Physicians
  - Independent practitioners
  - Nurses
  - Others

* Not limited to licensed or independent practitioners

Medical Records - Entries

- Provider should train personnel concerning proper entries.
  - e.g., form, content, method, timing
- Each entry should be:
  - legible to allow proper communication
  - complete
  - dated/timed
  - authenticated in written or electronic form
  - written in ink (preferably blue or black) or typed to ensure permanency and protect against alteration
  - specific, not general
  - objective and based on facts, not speculation
  - use quotations marks when quoting patient
  - use approved, standard abbreviations and symbols

42 CFR 482.24

Medical Records - Entries

- CMS Manual Interpretative Guidelines give further guidance.
  - Medical record considered complete if it contains sufficient info to identify patient; support the diagnosis/condition; justify the care, treatment and services; document course and results of care, treatment and services; and promote continuity of care.
  - Importance of timing and dating: necessary for patient safety and quality of care; establishes baseline for future actions; establishes timeline of events.
  - Must have method to establish identity of author of each entry.

Medical Records - Entries

- Must have method to require that each author takes a specific action to verify that entry is his/her entry, he/she is responsible for entry, and that entry is accurate.
- Authentication may include written signatures, initials, computer key or other code.
- When rubber stamps or electronic authorizations used, hospital must have policies/procedures to ensure stamps only used by individual whose signature they represent – no delegation.
- Insurers/payors may have policy prohibiting use of rubber stamps.

Medical Records - Entries

- For EMR, must demonstrate how it prevents alterations of record entries after they have been authenticated.
- Must be method of determining that the practitioner did authenticate the entry after it was created.
- Practitioner must separately date and time his/her signature even though there may already be a date/time on the document.
- If state law requires counter-signatures of supervisory staff on records made by residents or non-physicians, then policy should address counter-signature requirements and processes.

Medical Record – Four Key Points

1. Accuracy
   - information is relied on by others and could lead to improper medical advice
   - do not make entries for others
   - additions and corrections if done correctly
2. Completeness
   - do not leave blanks or gaps in chart
   - continue on next line; do not leave spaces.
   - do not start new form until lines on prior form are filled in or crossed out.
   - complete all fields by appropriate entry or "N/A".

Medical Record – Four Key Points

3. Relevance
   - do not use record to speculate, gripe, blame or complain
   - avoid criticism of other professionals in chart notes
   - avoid unsubstantiated subjective remarks
4. Timeliness
   - Entries should be made contemporaneously or as soon as possible after the event or observation.
   - Laws, regs or policies may require completion of record within certain time, e.g., 30 days.
   - More time = less reliable.
   - Never make entries in advance.
   - Never backdate entries

Medical Records – What If There Are Errors?

HOLLAND&HART

Medical Records – Additions or Corrections

- Late entries, corrections and amendments are okay so long as they are designated as such.

  (No one is perfect, not even physicians…)

- Accurate record more important than timing.

Medical Records – Additions or Corrections

- Errors and amendments should be done in a manner that preserves original entry.
  - Draw single line through error; designate it as "error"
  - Amendments should be initialed with date, time, title, and reason for change.
  - If the original document was in paper and scanned, need to reprint, fix and rescan.
  - Electronic documents should be corrected with an addendum labeled as such with date, time, title, and reason for change.
- Never erase, obliterate or delete prior entries.
  - Inference of bad conduct.
  - Potential claim for spoliation of evidence, tampering with evidence, obstruction of investigation, etc.

Medical Records – Additions or Corrections

- Correcting electronic documentation follows the same basic principles
  - system must have ability to track corrections or changes once it has been entered or authenticated
  - original entry must be viewable
- When a pertinent entry was missed or not written in a timely manner:
  - identify the new entry as "late entry"
  - enter the current date and time
  - document as soon as possible – the longer the time lapse, the less reliable the entry becomes

Medical Records – Additions or Corrections

- How to handle incomplete records when provider has left the practice/facility:
  - Send a letter informing provider of obligation under employment contract
  - Warn that medical staff membership or clinical privileges may be terminated if records are not completed by XX date
  - Report it to state licensing board – violation of duties
  - File lawsuit seeking injunction

Medical Records – Additions or Corrections

- Never amend or correct a medical record after receipt of notice of a potential claim.
- Obtain legal advice if charting errors are discovered following a complication or after a claim is threatened or filed.
- Deliberate alteration of medical records is illegal and unethical and may subject the writer to criminal and civil penalties.
- Technology is sophisticated.

Medical Records – Additions or Corrections

- Patients generally have a right to request an amendment to records in their designated record set.
- Covered entity may:
  - Require request to be in writing
  - Require explanation for request
- Provider must act in timely fashion.
  - Must respond within 60 days
  - May obtain 30-day extension if explain basis for extension in writing

45 CFR 164.526

HOLLAND&HART

Medical Records – Additions or Corrections

- If provider accepts amendment:
  - Make the amendment to the records
  - Attach or link requested amendment to relevant records
  - Notify individual of amendment
  - Seek permission to notify others regarding change
    - Persons identified by patient
    - Persons who may rely on prior record to the detriment of the patient, e.g., other doctors or business associates

45 CFR 164.526

Medical Records – Additions or Corrections

- Provider may refuse to make amendments if:
  - Provider did not create record unless person who created record is no longer available to act on the request
  - Record is outside the designated record set
  - Record is not subject to patient access, e.g., psychotherapy notes; risks outweigh benefits; promise of confidentiality to another; etc.
  - Record is accurate and complete

45 CFR 164.526

Medical Records – Additions or Corrections

- If provider denies amendment:
  - Denial must be in writing and explain—
    - Basis for denial
    - Right to attach copy of request or statement
    - Explain complaint procedures
  - Denial must be timely.
  - Provider may attach rebuttal statement to the individual's statement of disagreement.
  - Provider must attach or link patient's request.
  - Provider must provide the request or statement with any future disclosure.

45 CFR 164.526

HOLLAND&HART

Medical Records – Additions or Corrections

- Provider must:
  - Amend provider's own records if they receive notice of amendment from another covered entity
  - Document names and titles of persons responsible for receiving and processing requests for amendments
  - Retain the documentation as required by 45 CFR 164.530(j)

45 CFR 164.526

Medical Records – Control/Access

HOLLAND&HART

Medical Records – Ownership

- The provider/practice/facility owns the records.
  - Not the patient
  - Not other providers
- In case of institutional provider or practice, organizing documents, contracts or bylaws should specify who owns the records.
  - Specify who gets records upon termination or dissolution
  - Give practitioners reasonable access during or after termination of practice

HOLLAND&HART

Medical Records – Ownership

- Owner may generally:
  - Deny access unless laws provide otherwise
    - HIPAA
    - Medicare/Medicaid COPs
    - Subpoenas, orders, or warrants
    - Ethical or professional duties
- Owner may generally:
  - Charge a reasonable fee for providing access consistent with applicable law
    - HIPAA
    - Medicare/Medicaid
    - Subpoenas

HOLLAND&HART

Medical Records – Access Controls

- HIPAA requires that you have reasonable administrative, physical, and technical safeguards to protect access.
  - Secure rooms, computers, etc.
  - Monitor or control access
  - Log after-hours entries
  - Do not allow originals to leave facility

45 CFR 164.301, -.530

HOLLAND&HART

Medical Records – Retrieval and Charges

- Providers should have process that allows for prompt retrieval of relevant information.

45 CFR 164.301; 42 CFR 482.24

- HIPAA allows you to charge patient and personal rep a reasonable cost-based fee, which includes:
  - Cost of supplies and labor to copy info (e.g., paper, disc, etc.)
  - Cost of postage if patient requests mailing
  - Cost of preparing explanation or summary if patient requests summary and agrees to costs
  - Not cost of retrieval, handling, or processing the request

45 CFR 164.524

Medical Records – Retrieval and Charges

- HIPAA limits on charges only apply to disclosures to patients, not others, e.g.,
  - Other practitioners
  - Lawyers
  - In response to subpoenas
  - Insurers

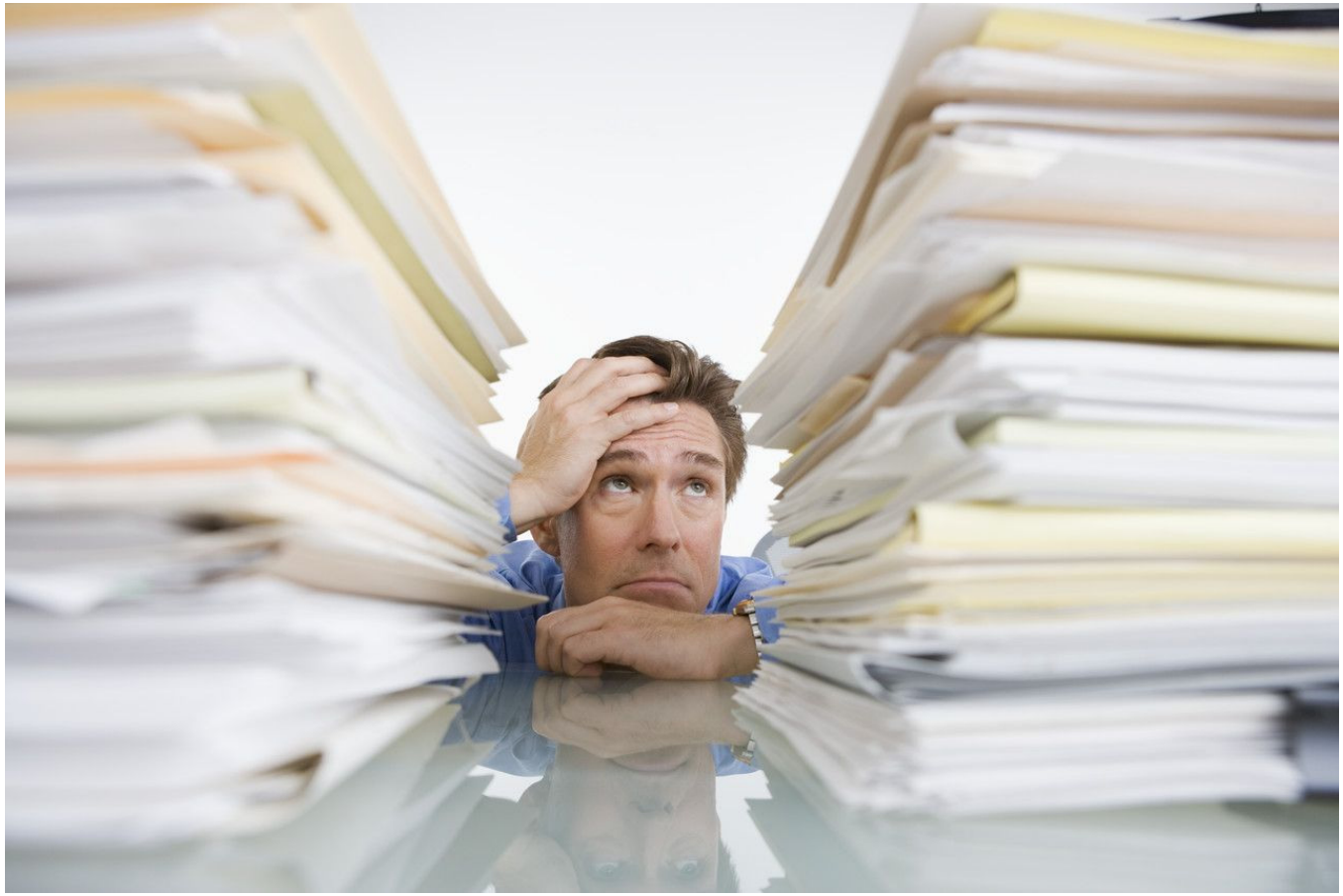
65 FR 82462, 82557; 67 FR 43182, 53254

- Subpoena rules generally allow you to charge a reasonable fee.
- State laws/regs may limit fees.
- Payor contracts may limit charges or fees.

Medical Records – Retrieval and Charges

- Suggestions:
  - Establish policies and schedules for charges to:
    - Patients
    - Practitioners
    - Payors
    - Others
  - Notify patients and others of charges in advance.
    - Notice of privacy practices
    - At time of request
  - Negotiate charges in payor contract negotiations.
  - Generally require payment before production.
  - Periodically reevaluate charges.

Medical Records – Where Do They Go?



HOLLAND&HART

Medical Records – Retention

- Need to establish written retention and destruction policy/schedule – why?
  - Facilitate patient care
  - Comply with relevant statutes, regs, contracts, accreditation standards
  - OIG Compliance Guidance recommends proper record retention policy
  - HIPAA security rules require it for e-PHI
  - Help establish defense against claim or allegation of improper destruction of records

Medical Records – Retention

- At a minimum, retention policy must:
  - Ensure patient health information is available to meet the needs of continued patient care, legal requirements, research, education and other legitimate uses
  - Include guidelines that specify what information is kept, the time period, the storage medium, storage location
  - Include clear destruction policies and procedures that include appropriate methods of destruction
  - Designate a person to be responsible for deciding what to keep and destroy
  - Log the records that have been destroyed, including date and method
  - Employee training

Medical Records – Retention

- In establishing record retention policy, consult:
  - Medical staff
  - Attorneys
  - Risk managers
  - Liability insurance carrier
  - Medical record director
  - Administrator

Medical Records – Retention

- No single standardized record retention schedule that organizations/providers must follow.
- Depends on:
  - Patient care needs
  - Statutory and regulatory requirements, e.g.: Medicare/Medicaid: 5 years for hospitals and 6 years for CAH (42 CFR 482.24(b))
  - HIPAA privacy regs require 6 years from creation or the date when it was last in effect, whichever is later (45 CFR 164.530(j))
  - Accreditation standards
  - Contract terms
  - Insurance and risk management concerns
  - state medical board policies, e.g.: Colorado Policy 40-07 recommends 7 years for adult and 7 years past majority for minor

Medical Records – Retention

- In the absence of specific state requirements, keep health information for at least the period specified by state's statute of limitations.
- Relevant statutes of limitation:
  - Malpractice
    - Generally 2 years from event but check state statute
    - Might be extended if foreign object left in body or malpractice concealed
    - Tolled due to minority or incompetency
  - Breach of Contract
    - Longer than malpractice
    - Different limits for written and oral contracts

Medical Records – Retention

- Relevant statutes of limitation if Medicare/Medicaid involved:
  - False Claims Act: later of
    - 6 years from date of violation, or
    - 3 years after government had notice but no later than 10 years from date of violation.

  31 USC 3729, 3731(b)

  - Civil Monetary Penalties: 6 years from date the claim was presented.

  42 CFR 1003.132

Medical Records – Retention

- The Association of Health Information recommends a minimum of 10 years.
- Defense attorneys recommend that records be retained forever – hard to defend without records.
- A study completed in 2008 finds that many hospitals keep records permanently – the next most frequent standard was 20 years.
- Miscellaneous things to remember:
  - Retention or destruction policy should be suspended immediately for any records relevant to any threatened or pending government investigation or litigation.
  - If using an outside entity to assist with records retention or destruction, must have HIPAA-compliant business associate agreement.

Medical Records – Retention

- A bit off topic, but what about retention of credentialing files?
  - best to keep them forever
  - if cannot keep forever, keep for at least five years after retirement or death (if physician practicing at time of death)
  - still could be issues – especially with obstetricians – statute of limitations for minors
    - age of majority plus two years
  - keeping forever protects against negligent credentialing claims as it is hard to defend against claim without credentialing file
  - beneficial to physicians to keep them forever as some licensing authorities want credentialing documentation for all hospitals at which the physician applicant has ever been credentialed
  - is there a way to scan and store electronically?

Medical Record – Retention

http://library.ahima.org/PB/RetentionDestruction#.V-NckfkrK_4

Appendix A: Federal Record Retention Requirements

Type of Documentation	Retention Period	Citation/Reference
Abortions and related medical services documentation	Maintain for three years.	42 CFR 50.309
Ambulatory surgical services	Retention periods are not specified	42 CFR 416.47
Clinics, rehabilitation agencies, and public health agencies as providers of outpatient physical therapy and speech-language pathology services	As determined by the respective state statute, or the statute of limitations in the state. In the absence of a state statute, five years after the date of discharge; or in the case of a minor, three years after the patient becomes of age under the state law or five years after the date of discharge, whichever is longer.	42 CFR 485.721 (d)
Clinics, rural health	Six years from date of last entry and longer if	42 CFR 491.10 (c)

Medical Record – Retention

http://library.ahima.org/PB/RetentionDestruction#.V-NckfkrK_4

Appendix B: Accreditation Agency Retention Standards

Accreditation Agency	Retention Standard	Reference
Accreditation Association for Ambulatory Health Care (AAAHC)	Requires organizations to have policies that address retention of active clinical records, the retirement of inactive clinical records, and the retention of diagnostic images.	*Accreditation Handbook for Ambulatory Care*
American Accreditation Healthcare Commission/URAC	Member Protection Standard #7 states "the network shall have storage and security of confidential health information, access to hard copy and computerized confidential health information; records retention; and release of confidential health information."	*Health Network Accreditation Manual*
CARF...the Rehabilitation	Requires organizations to have policies that address record retention.	*Adult Day Services*

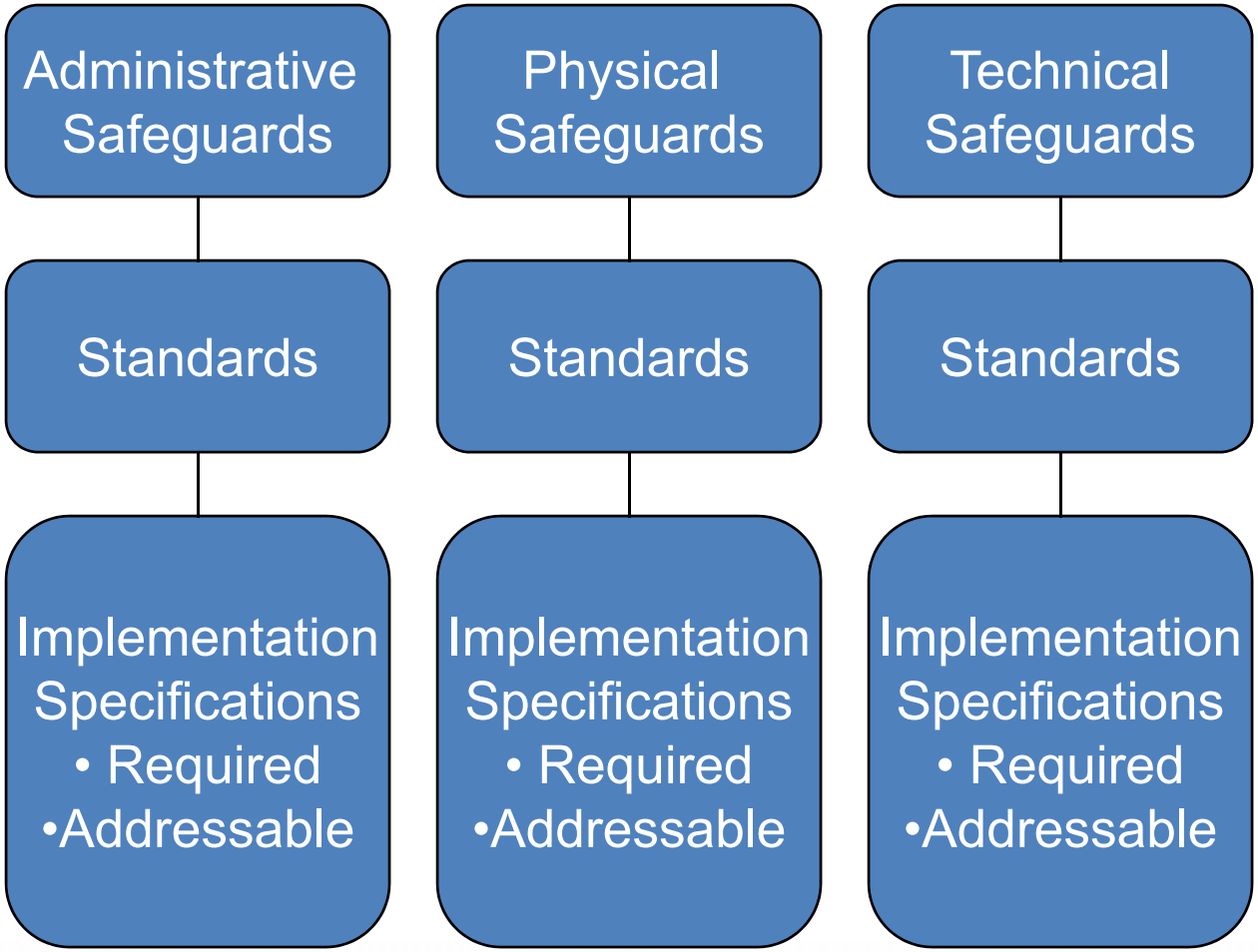
Medical Records - Storage

- Must be stored in safe and secure environment
  - ensure physical integrity
  - safeguard against improper access, tampering, defacement
  - ensure confidentiality
- Must be readily available and producible
- Reasonable steps taken to ensure protection from theft, loss and unauthorized use or disclosure
- Keep paper records in restricted access areas or locked filing cabinets
- Do not allow record to be removed from facility without subpoena or court order

Medical Records - Storage

- Move to off-site storage after reasonable time, e.g., 3 to 5 years after last date of service.
- Use sign-out system when record removed from storage.
- Establish system to allow proper retrieval.
- Implement administrative, physical and technical safeguards to limit improper intentional or inadvertent disclosures.

EMR – Security Rule: Safeguards (45 CFR 164.308-.312)



HOLLAND&HART

EMR – Security Rule: Safeguards

- "Required": implement the specification.
- "Addressable":
  - Assess reasonableness of specification.
  - If spec is reasonable, implement it.
  - If spec is not reasonable,
    - Document why it is not reasonable (e.g., size, cost, risk factors, etc.), and
    - Implement alternative if reasonable.
- Must review and modify as needed.

EMR – Security Rule: Safeguards

- Not technologically specific to accommodate technological advances.
- May use measures that reasonably allow you to comply with standards considering:
  - Size, complexity and capabilities,
  - Technical infrastructure, hardware and software,
  - Costs,
  - Probability and criticality of risks.

EMR– Security Rule: Administrative Safeguards (164.308)

- Assign security officer.
- Implement policies, procedures and safeguards to minimize risks.
- Sanction workforce members who violate policies.
- Process for authorizing or terminating access to e-PHI.
- Train workforce members on security requirements.
- Process for responding to security incidents.
- Review or audit information system activity.
- Establish backup plans, disaster recovery plans, etc.
- Periodically evaluate security measures.

EMR – Security Rule: Physical Safeguards (164.310)

- Limit access to physical facilities and devices containing e-PHI.
- Document repairs and modifications to facilities.
- Secure workstations.
- Implement policies concerning proper use of workstations.
- Implement policies concerning the flow of e-PHI into and out of the facility.
- Implement policies for disposal of e-PHI.
- Create a backup copy of e-PHI.

EMR – Security Rule: Technical Safeguards (164.312)

- Assign unique names or numbers to track users.
- Implement automatic logoff process.
- Use encryption and decryption, where appropriate.
- Implement systems to audit use of e-PHI.
- Implement safeguards to protect e-PHI from alteration or destruction.
- Implement methods to ensure e-PHI has not been altered or destroyed.
- Implement verification process.
- Protect data during transmission.

HOLLAND&HART

EMR – Security Rule: Documentation

- Implement written policies and procedures to comply with standards and specs.
- Maintain documentation in written or electronic form.
- Required
  - Maintain for 6 years from later of creation or last effective date
  - Make documents available to persons responsible for implementing procedures
  - Review and update documentation periodically

Medical Records - Destruction

- Destruction must be carried out in accordance with federal and state law.
- Records involved in any open investigation, audit, or litigation must not be destroyed until the litigation case has been closed.
- As with record retention, there is no single standard destruction requirement.
- Some states require organizations create an abstract of the destroyed patient information, notify patients when destroying patient information, or specify the method of destruction used to render the information unreadable.

Medical Records - Destruction

- Unless state law to the contrary, organizations must ensure records are destroyed with a method that provides for no possibility of reconstruction of information.
  - Paper record methods of destruction include burning, shredding, pulping, and pulverizing
  - Microfilm or microfiche methods of destruction include recycling and pulverizing
  - Laser discs used in write once-read many document-imaging applications are destroyed by pulverizing
  - Computerized data are destroyed by magnetic degaussing
  - DVDs are destroyed by shredding or cutting
  - Magnetic tapes are destroyed by demagnetizing

Medical Records - Destruction

- Must maintain documentation of the destruction of health records permanently and include the following:
  - Date of destruction
  - Method of destruction
  - Description of the disposed records
  - Inclusive dates
  - Statement that records were destroyed in normal course of business
  - Signatures of individuals supervising and witnessing destruction
- Ethical statements sometimes require that notice be given to the patient – generally, no legal requirement to contact patient before records destroyed (except in bankruptcy)

Medical Records - Destruction

- Under the HIPAA privacy rule (45 CFR, Parts 160 and 164), when destruction services are outsourced to a business associate the contract must provide that the business associate will establish the permitted and required uses and disclosures and include the following elements:
  - The method of destruction or disposal
  - The time that will elapse between acquisition and destruction or disposal
  - Safeguards against breaches
  - Indemnification for the organization or provide for loss due to unauthorized disclosure
  - Require the business associate to maintain liability insurance in specified amounts at all times

Medical Records - Transfer

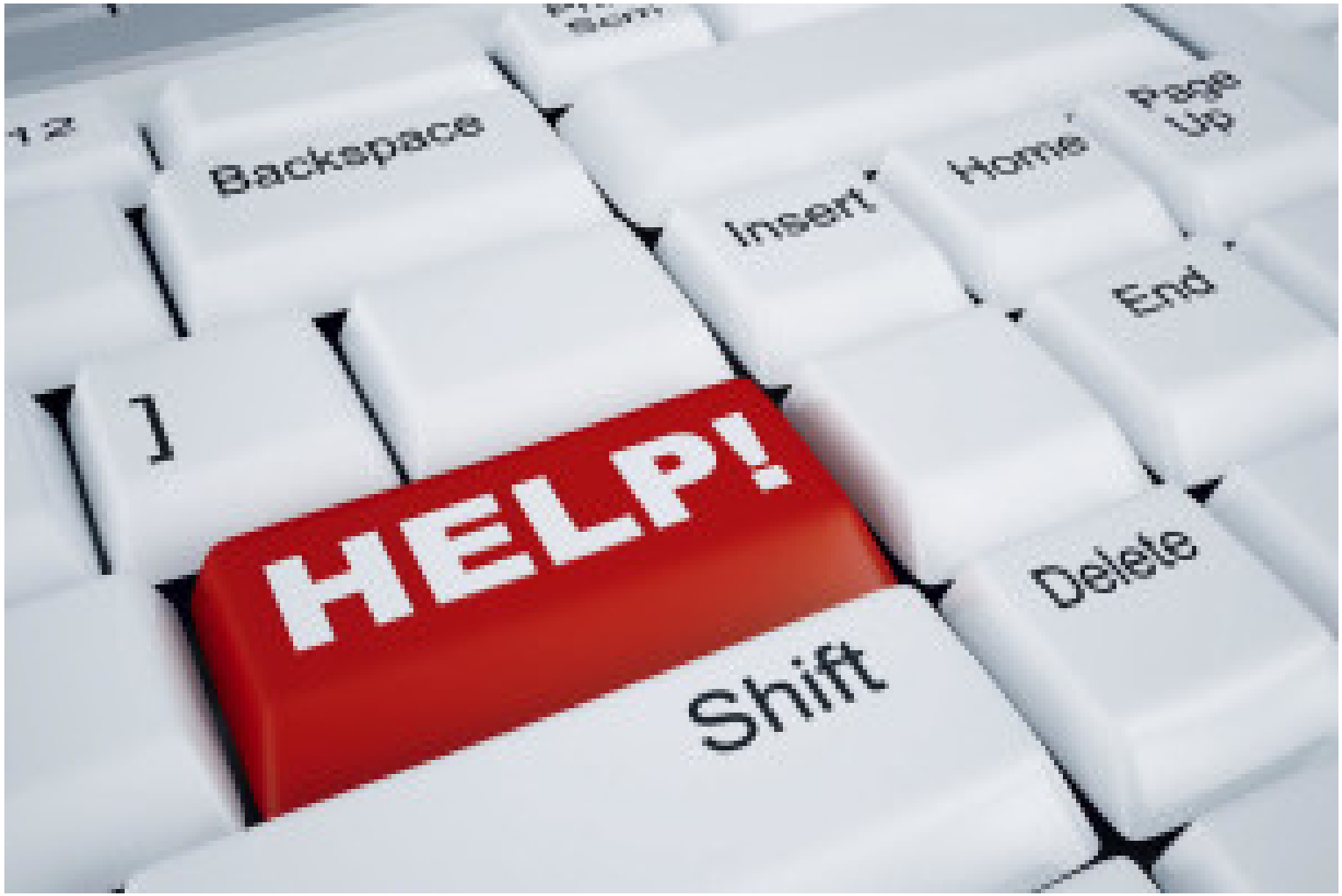
- Physician selling practice may designate purchaser as custodian of records.
- Cannot "sell" the records.
- Cannot "transfer" patients to the purchasing physician's practice.
- Patients have right to select any physician they chose.
- Purchase contract should specify that buyer will:
  - be custodian of records
  - maintain records in safe place
  - make copy available for transfer to new physician and make the records available for selling physician if needed for defense
  - hold records for XX years – no destruction prior without consent

Medical Records – End of Practice

- Physician or physician group practice is responsible for making appropriate arrangements for disposition of records when practice closes.
- Physicians turning practice over to replacement physician should have agreement that stipulates the recommended retention time and access capability.
- When a practice closes and medical records are transferred, patients should be notified that they may designate a physician or other provider to receive their records.
- If patient does not designate a physician, records may be transferred to a custodian.

HOLLAND&HART

Additional Resources



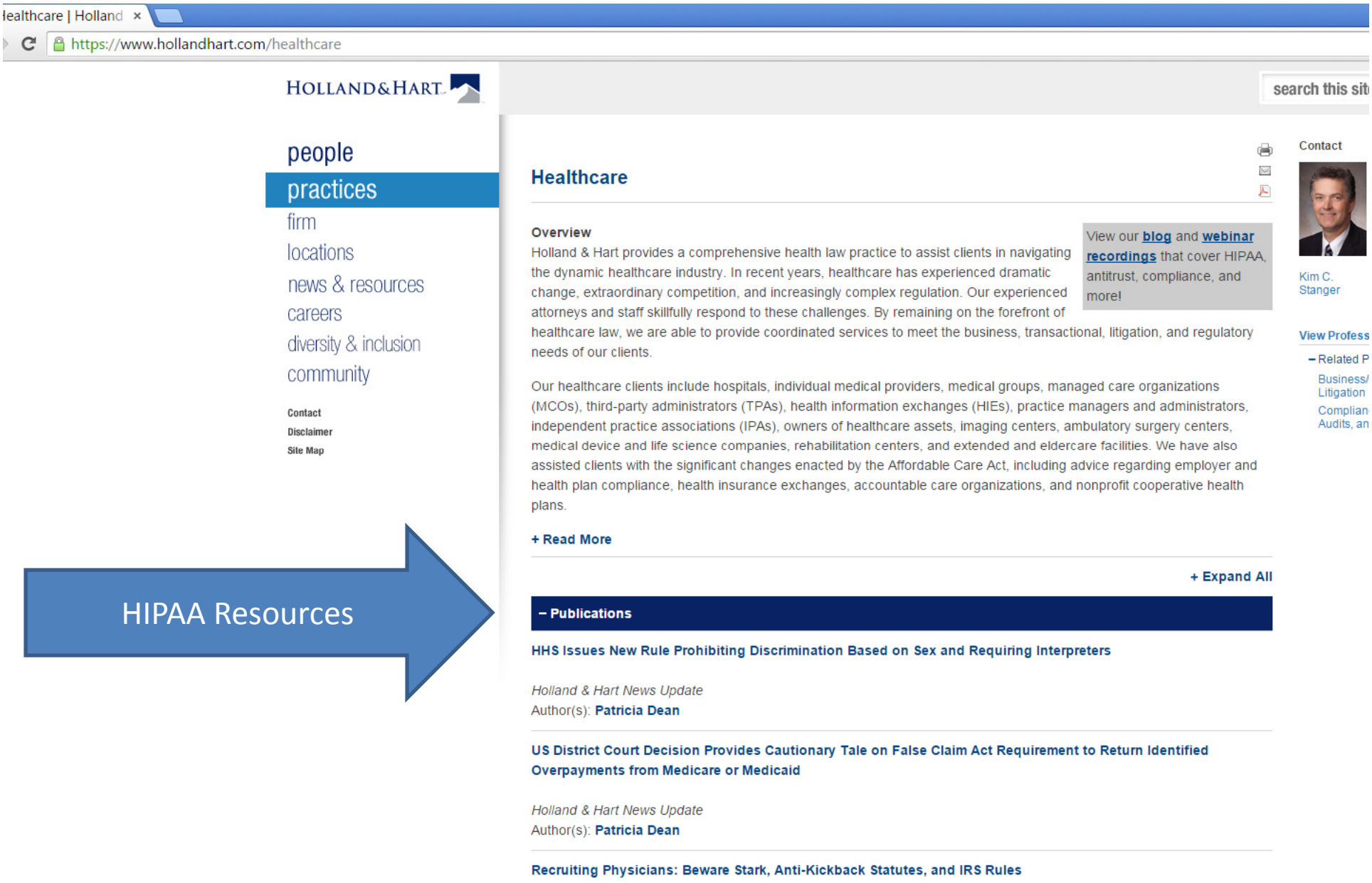
HOLLAND&HART

Additional Resources

- American Health Information Management Association (www.ahima.org)
- 42 CFR 482.13
- 42 CFR 482.24
- 45 CFR 165.524
- 45 CFR 164.526
- 45 CFR 164.530

HOLLAND&HART

Holland & Hart Website



HIPAA Resources

Additional Resources

- *Health Law Basics* monthly webinar series
  - Past webinars available at www.hhhealthlawblog.com
  - Telemedicine (July 2015)

- *Healthcare Update* and *Health Law Blog*
  - Under "Publications" at www.hollandhart.com.
  - E-mail me at tlocke@hollandhart.com

HOLLAND&HART

Questions?

Teresa D. Locke

Holland & Hart LLP

tlocke@hollandhart.com

(303) 295-8480

HOLLAND&HART