Questions
Case Studies – Work Plan Priorities

Credentialing, Privileging, Peer Review
FTCA
HIPAA
Privacy/Security
Back Up/Disaster Recovery
Records Management
Provider Closure
Patient Access
Credentialing

What is Credentialing?

The process of verifying that a licensed/certified healthcare practitioner is currently qualified to practice in his/her profession. The “paper” piece

- Training
- Education
- Certifications
- Licensure
- DEA number
- Health record
- Immunizations
- National Practitioner Data Bank (NPDB)
Privileging

What is Privileging?

Assessment of providers’ education, training, and developed skills that contribute to the provision of patient care within the health center’s scope of practice

What is Clinical Competence?

The capability to perform acceptably those duties directly related to patient care. Includes:

- Professional behavior
- Clinical skills
- Medical knowledge

Medical staff cannot provide health care prior to completion of credentialing and privileging process.
Credentialing vs. Privileging

What is the Difference Between Credentialing and Privileging?

**Credentialing**
- Step 1 of the process
- Vetting the provider
- “Paperwork” (e.g., licensing, education)

**Privileging**
- Step 2 of the process
- Authorizing the provider’s scope of practice
- Within health center scope of services
- “Skills and abilities” (e.g., competence, specialized training)
Peer Review

What is Peer Review?

• Process that evaluates the quality and performance of healthcare ordered or provided by licensed independent practitioners
• Goal is to prevent harm to patients and improve the quality of healthcare
• Specific, formal, targeted
• Protected by state laws
Credentialing – Case Study

Nurse Imposters, Texas

• Allegedly, a 33-year-old female stole the identity of an RN in order to get nursing jobs at eight different hospice companies from 2009 to 2012. Records show she was responsible for the care of more than 160 patients during that time.

• A man faked being a nurse for at least a decade. The imposter pleaded guilty to practicing nursing without a license, tampering with a government document, and aggravated perjury. Ironically, he was promoted to clinical services director before being fired following a tipster’s call.
Work Plan Priority Issue #1: FTCA

- Priority Issue for Health Center Compliance Work Plan

- Coverage dependent on compliance with statute, regulations, and attestations
Health Center has attested that it has:

1. Clinical Protocol
2. Medical Records P/P
3. No Show Management
4. Patient Triage
5. Tracking Systems
   a. Referral
   b. Hospital
   c. Diagnostic

6. Risk Management Plan
FTCA- Clinical Protocols

There are clinical protocols that define appropriate treatment and diagnostic procedures for selected medical conditions.

- Clinical protocols for frequent conditions (i.e. diabetes, hypertension, pain management, prenatal care, etc.).
- Protocols need to be based on standard of care for that type of practice.
- Protocols need to be updated periodically.
- Providers and clinical staff need orientation and training regarding their role of standard of care.
- Clinical procedures done at the health center are clearly defined, staff is qualified to perform the procedures.
- Peer reviews are conducted based on clinical protocols.
Medication errors are often the cause of Adverse Patient Events, clinical risk management policies help prevent harm to patients by ensuring these types of errors are prevented.

An example of an adverse medication error would be a provider prescribing an in-office injectable medication such as a Depo-Provera shot and the wrong injectable, a flu shot was given instead. Four months later, the patient was pregnant.
FTCA- Medical Records

There are medical record policies and procedures that address the following:

Privacy (HIPAA) – YES or NO
Completeness of documentation – YES or NO
Archiving Procedures – YES or NO

Medical records are periodically reviewed to determine quality, completeness, and legibility
FTCA- “No Show”

“No-Show” risks are:
- Possible negative health consequences for patients
- Liability risk
- Reduced accessibility
- Lost revenue

- Patients need to be informed of health center policies and procedures for missed appointments; follow-up for missed appointments should be documented in patient records, reasonable accommodations for missed appointments needs to be considered.

- Tracking and monitoring no show appointments helps explore the causes (i.e. internal and external), and patient utilization patterns.
FTCA- Patient Triage

There are policies/procedures that address the following Patient Triage:

- Triage – YES or NO
- Walk-in Patients – YES or NO
- Telephone Triage – YES or NO
- No Show Appointments – YES or NO
FTCA- Patient Triage

Triage policies include who, what, when and how to respond.

Depending on the type of practice, (e.g. family practice, OB, pediatrics, etc.) standard of care for different patient conditions/compliant warrants different triage responses. Staff roles and responsibilities are clearly identified. Staff are trained in their duties and responsibilities. Triage events are part of the QA/QI processes.
FTCA- Tracking System

There is a tracking system for patients who require follow-up of referrals, hospitalization, diagnostics (i.e. x-ray, lab results)

Referral tracking – YES or NO
Hospitalization tracking – YES or NO
Diagnostic testing (x-ray, labs) – YES or NO
Does referral policy ensure referrals are:

• all patient referrals are documented
• all calls and contacts are documented
• tracked, by whom, how often and within a specific time frame
• referring providers are contacted for patient information
• patients are reminded of the importance of making referral and are called to be reminded of the referral appointment
• referring providers notify health center if patient ‘No shows” for the referral
FTCA – Referral Tracking

Does referral policy ensure referrals are:

• patients are contacted if they do not make their appointments
• Include documentation in chart with results of referrals
• the health center uses their EHR to assist with tracking referrals (reports are generated daily/weekly/monthly)
• Referral tracking monitoring is part of QA/QI processes
FTCA- Hospital Tracking

• The overarching goal is to deliver health care services early/timely/consistently so that hospitalizations and/or ED visits are less. When a patient is hospitalized once released, the goal is to maintain and improve their health status.

• Being discharged from the hospital can be dangerous

• 20% of patients experience adverse events within 3 weeks of discharge

• Nearly three-quarters of which could have been prevented

• Adverse drug events are the most common post discharge complication nearly 40% of patients are discharged with pending test results and recommended further diagnostic testing

FTCA – Diagnostic Tracking Policy

The Diagnostic Tracking policy should include the following information:

• A process for tracking laboratory and imaging referrals;
• Designation of one person or team responsible for assuring receipt of care;
• Time frame for follow up for results; and
• Documentation in the medical record
• Information related to how many and what type of attempts will be made when trying to contact the patient.
FTCA – Diagnostic Tracking Policy

The Diagnostic Tracking system at a minimum should ensure that the following details are recorded:

• Patient information;
• Date test ordered;
• Ordering provider;
• List of tests ordered;
• Date results received;
• Provider who reviewed results;
• Follow up recommendation; and
• Communication of results to patient.
FTCA- Diagnostic Tracking Policy

Why is this important?

Missed or delayed diagnoses (particularly cancer diagnoses) are a prominent reason for malpractice claims.

• The organization must identify normal, abnormal and critical lab values.
• Health center staff must know policies and procedures for abnormal and critical lab results and individual’s identified role.
• Provider notification of all labs, needs to include EHR if appropriate.
• Policies and procedures need to describe how often are labs reviewed, what happens when the ordering provider is not on-site.
FTCA- Diagnostic Tracking Policy

• Immediate patient notification of all CRITICAL test results. In some areas these are known as “Panic” values.
• Procedures need to include after hours, weekend and holiday responses to abnormal lab values.
• Patient records need to include documentation and treatments rendered.
• Documentation of notification [date/time/person spoken with] and follow up recommendations including come to the health center or go to the emergency room.
FTCA-Diagnostic Tracking Policy

• What happens if the patient can’t be reached.
• **DO NOT** leave critical or abnormal lab results on voicemail or text or email. Have alternative patient contact information. Verify patient information at each contact with the patient (phone and/or appointment).
• In some cases law enforcement offices can be called for “sick visit”.
• The diagnostic tracking log is complete and up to date, the tracking information is part of the patient record.
Provider fails to notify 32y/o F of abnormal diagnostic test results, fails to inform the patient further testing is needed---resulting in later diagnosis of breast CA and Right breast mastectomy
FTCA - 2018

EHB will open for applications to be filed
June 23, 2017 – July 24, 2017

Decisions will be made within 30 days of receipt of a “complete” application

Some changes from the previous application

• Significant new emphasis on risk management including applicants risk management program, policies, training, and board involvement.

• Risk management operating procedures must be described in detail.

• At a minimum, training must address obstetric related issues, infection control, and HIPAA.
FTCA-Risk Management Plan

**Environment:** Buildings and grounds, equipment, materials, disaster preparation and management, safety/security, event/incident/accident reporting and investigation.

**Human resources:** HR policies and procedures, compliance with employment regulatory requirements, job descriptions, employee handbooks, employment contracts, employee credentialing, employee orientation, employee health, on-going employee training and development, document security and retention.
FTCA-Risk Management Plan

**Information technology**: Privacy and security, vendor contracts, HIPPA, HITECH, information exchanges, patient portals, disaster and recovery plans, IT system redundancy plans.

**Clinical**: Credentialing of providers, quality/performance assessment and improvement, standard of care (clinical protocols), environmental and employee safety, infection control, patient tracking and follow-up, patient communications, patient and family education, patient satisfaction, pharmaceuticals and therapeutics, behavioral health and social service programs, volunteers.
FTCA-Risk Management Plan

• Governing Board has a commitment to safety and quality;
• The plan is based on healthcare national standards and regulatory/program requirements
• The plan is customized to fit the organization’s, sites, services, size, and patient population
• There is a clear mission statement with goals, objectives, activities, timelines, and defined staff responsibilities
• The plan is reviewed and updated periodically
• There is active and on-going monitoring/auditing, problem identification, data collection, corrective actions, documentation and reporting to the committee and the Board of Directors
• The health center engages all staff in risk management
Work Plan Priority Issue #2: HIPAA

**HIPAA** – statutory, regulatory, HRSA Program Requirements, attestation under MU Program

1. Protecting, Helping, Informing
2. Privacy and Security
3. Designated Record Set
4. Risk Assessment
5. Back up and Disaster Planning
6. Medical Records and Documentation Standards
ONC-HIPAA

• PHI must be kept private
• Only Discuss information for work purposes
• Think about where you are and who can overhear you
• Think before you share PHI verbally
• The Same HIPAA rules apply for PHI in conversations as in written or electronic formats
• PHI can only be looked at for business purposes
• Only access the Minimum Necessary amount of PHI to get your job done
• Everything else must be kept secure
• PHI can be shared over the phone when appropriate
• Take steps to verify who is on the phone
ONC- HIPAA

Privacy and Security

• Keep PHI Private and Secure by following the “2 Key rule”
• When not supervised PHI should always be behind 2 “locks” to prevent unauthorized access
• Protecting your computer also protects PHI and other sensitive data
• Use Virus Protection
• Don’t open email attachments from unauthorized senders
• Never download programs from the internet
Designated Record Set:
The HIPAA privacy rule defines the **designated record set** as a group of records maintained by or for a covered entity that may include patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions.

Under HIPAA, the **designated record set** is used to clarify the rights of individuals to access, amend, restrict, and acquire an accounting of disclosures. Individuals have the right to inspect and obtain a copy, request amendments, and set restrictions and accountings of medical and billing information used to make decisions about their care.
ONC- Privacy & Security

• **Risk** - the probability or threat of damage, liability, loss or other negative occurrence that is cause by external or internal vulnerabilities

• **Risk Assessment** – identification, evaluation, and estimation of the levels of risk involved in a situation, their comparison against benchmarks or standards, and determination of acceptable level of risk

• **Risk Management** – identification, assessment and prioritization of risk followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of information events or to maximize the realization of opportunities
ONC- Privacy & Security

• **Threat** – a person or thing likely to cause damage or danger: any circumstance or event with the potential to adversely impact organizational operations

• **Vulnerability** - the inability to withstand the effect of a hostile environment

Risk = F (likelihood of a given threat triggering or exploiting a particular vulnerability & resulting impact on the organization

A risk assessment will identify potential threats to and vulnerabilities of PHI and the associated risk

NOTE: a threat must have the capability to trigger or exploit a vulnerability to create risk
Agencies should develop appropriate protective measures for their records and copies of their vital records to respond to actual or potential emergencies or disasters identified in contingency planning. This is the records management aspect of emergency management. Vital records are emphasized because they tend to have the greatest value in case of emergency or they require extra protection because they document legal or financial rights. The type and level of value determine the amount of protection agencies should provide. Special protective measures for vital records may include using fire-rated filing equipment for storage; constructing onsite vaults; transferring records to offsite storage; duplicating the records at the time of their creation, such as computer "backup" tapes, using existing duplicates as vital record copies; or microfilming vital records.
ONC- Backup/Disaster Planning

Additional protective measures are needed for Federal records maintained on a medium other than paper. These "special records" require specific environmental conditions and careful handling throughout their life cycle to ensure their preservation. Agencies must maintain temperature and humidity controls for special records such as photographs and negatives, microforms, audio and video tapes and disks, and electronic tapes and disks.
ONC- Disaster Recovery Plan

• Table of Contents
• Introduction
  • use of the document
  • how it is to be revised
  • responsible personnel
  • general information about the facility
• . Emergency information sheet
  • fire/police departments
  • hospitals
  • emergency shut-off
  • utility companies
  • brief list of emergency respondents
• Telephone/reporting tree
ONC- Disaster Recovery Plan cont.

• Records priorities
• Response outline
  • lead personnel responsibilities
  • assessing the situation
  • organizing/prioritizing efforts
  • establishing a command post
  • eliminating hazards
  • controlling the environment
  • dealing with the media
  • obtaining emergency funding/supplies
  • providing security
  • providing human comforts
  • training in salvage techniques onsite
• Supply lists and assistance/equipment vendors
• Clear description of salvage techniques
• Rehabilitation plans for conservation treatment
ONC- Disaster Planning Steps

• Identify and assign responsibility (committees, task forces, or teams)
  • planning
  • response
  • recovery

• Train members of the committees, task forces, or teams

• Conduct a risk analysis
  • identify potential building problems
  • survey fire protection policies and equipment
  • assess ability to protect people
  • evaluate potential for damage from natural disasters

• Establish goals and a timetable

• Develop a reporting schedule and reporting lines
ONC- Disaster Planning Steps cont.

• Evaluate records and assign priorities
• Identify potential sources of damage
• Assess prevention and protection needs
  • stockpile supplies and equipment
  • replenish when necessary
• Review fiscal implications
• Prepare the plan
• Distribute the plan
  • train
  • drill
• Evaluate the plan and update it regularly
ONC- Backup/Disaster Review & Testing

• The records disaster recovery program coordinator should conduct a periodic review of the records recovery plan with the assistance of selected agency officials to determine its adequacy and accuracy. This review should include the list of vendors (with telephone numbers, addresses, and other relevant data) that may have to be called upon in case of an actual records emergency or disaster.

• The plan should also be periodically tested, much as fire drills and building evacuation procedures are tested. The test should include the records disaster recovery team and evaluate its activities as well as the usefulness and thoroughness of the recovery plan. Modifications to either the plan or to the team's responsibilities should be made as needed.
Medical Records and Documentation Standards

Medical record standards reflect the importance of confidentiality and accessibility by authorized users only.

You are required to:

• Keep a unique, individual record for each patient
• Establish an organized record-keeping system to ensure that medical records are easily retrievable for review and available for use when needed, including at each patient visit
• Store and maintain medical records in a centralized and secured location accessible only to authorized personnel and provide equivalent security for electronic medical records
• Maintain and organize documents within medical records in a specified order
• Ensure that documents are fastened securely within a paper medical record
• Provide periodic training in confidentiality and security for patient information
Medical Records and Documentation Standards

The following concerning documentation is required:

• Member identifiers appear on every piece of documentation
• Entries are legible to others and are recorded in black or blue ink if on paper
• Entries are dated and authenticated by the author
• Documentation is made at the time service is provided
• Documentation must support all codes submitted
• Only standard medical abbreviations should be used in documentation
• All patient encounters, including telephone, fax, and electronic message exchanges are documented
• Documentation of any advance directives is in a prominent part of a member's medical record and includes whether or not a member has executed an advance directive, as well as documentation of any information about advance directives that was made available to the member
Medical Records and Documentation Standards

Documentation must include the following content:

- Problem list, including significant illnesses and medical conditions
- Medications
- Adverse drug reactions
- Allergies
- Smoking status
- Any history of alcohol use or substance abuse
- Biographical or personal data
- Pertinent history
- Physical exams
Medical Records and Documentation Standards cont.

• Documentation of clinical findings and evaluation for each visit
• Laboratory and other studies that signify review by the ordering provider
• Working diagnoses consistent with findings and test results
• Treatment plans consistent with diagnoses
• A date for return visits or a follow-up plan for each encounter
• Previous problems addressed in follow-up visits
• A current immunization record
• Preventive services and risk screening
AHIMA- EMR Policy

Sanctions imposed for privacy and security violations must be consistent across the organization, regardless of the violator's status, with comparable discipline imposed for comparable violations. Organizational policy should address sanctions related to violations of both state and federal regulations as well as internal privacy and security policies. The policy should also address how the sanctions support the organization's human resource corrective action policy.
AHIMA- EMR Policy

Organizations must establish general principles and processes that lead to fair and consistent outcomes, including the following:

• The policy and procedures should be developed, documented, and approved by organizational leadership including legal, compliance, risk management, human resources, medical staff services, and others as applicable.

• The policy should be written in a format that can accommodate ongoing updates to reflect modifications to the regulations, accreditation standards, and other organizational policies, including, but not limited to federal regulations (i.e., HIPAA, HITECH), state regulations (i.e., data breach notification laws, health codes), and accreditation standards (i.e., Joint Commission).

• The policy should be aligned with other related organizational policies and contracts to ensure consistency across the organization, including, but not limited to, human resources policies and contracts, medical staff bylaws and rules and regulations, union contracts, vendor contracts, and business associate agreements.

American Health Information Management Association
AHIMA- EMR Policy

• The policy should be subject to defined oversight with defined reporting responsibility. A possible model would include an ad-hoc sanctions committee that reports to the privacy and security committee, which in turn reports to the compliance and oversight committee, and up to the audit and compliance committee of the board of trustees.

• The policy should be communicated and accessible to all workforce members (i.e., posted on the organization's intranet, available in policy manual, distributed to staff, and featured in workforce training).

• The policy should address the appropriateness of applying the HITECH breach notification sanctions process if it is determined that unauthorized access, use, disclosure, or destruction has occurred.
AHIMA- EMR Policy
The policy should address investigations of disclosures made by workforce members who are whistleblowers or victims of a crime as potential nonviolations. Examples of these types of disclosures include, but are not limited to, a workforce member acting on good faith who:

• Believes that the organization has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or believes that the care, services, and conditions provided by the organization potentially endangers one (or more) patients, workforce members, or other members of the general public.
AHIMA- EMR Policy

• Discloses PHI to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of the organization
• Discloses PHI to an appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the organization
• Discloses PHI to an attorney retained by or on behalf of the workforce member for the purpose of determining legal options regarding disclosure conduct
## Meaningful Use Core Objectives

<table>
<thead>
<tr>
<th>Provide clinical summaries for patients for each office visit</th>
</tr>
</thead>
<tbody>
<tr>
<td>What this measure requires</td>
</tr>
<tr>
<td>What that means for you</td>
</tr>
<tr>
<td>Are you excluded from doing this?</td>
</tr>
</tbody>
</table>
# Meaningful Use Core Objectives

<table>
<thead>
<tr>
<th>Protect electronic health information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What this measure requires</strong></td>
</tr>
<tr>
<td>Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1), including addressing the encryption/security of data at rest and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.</td>
</tr>
<tr>
<td><strong>What that means for you</strong></td>
</tr>
<tr>
<td>You have to meet the same HIPAA requirements for protecting patient information in your EHR as you do for paper records. To do this, you must conduct a security review of your system and correct any problems that could make patient information vulnerable.</td>
</tr>
<tr>
<td><strong>Are you excluded from doing this?</strong></td>
</tr>
<tr>
<td>There are no exclusions. Everyone must meet this objective.</td>
</tr>
</tbody>
</table>
# Meaningful Use Core Objectives

<table>
<thead>
<tr>
<th>Provide patients the ability to view online, download and transmit their health information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What this measure requires</strong></td>
</tr>
<tr>
<td>• More than 50% of all unique patients are provided online access to their health information within 4 business days after the information is available to the EP.</td>
</tr>
<tr>
<td>• More than 5% of all unique patients view, download or transmit to a third party their health information.</td>
</tr>
<tr>
<td><strong>What that means for you</strong></td>
</tr>
<tr>
<td>Not only do you have to provide online access to health information for over half of your patients, you also have to make sure that more than 5% of your patients actually access the online health information you have made available.</td>
</tr>
<tr>
<td><strong>Are you excluded from doing this?</strong></td>
</tr>
<tr>
<td>You can be excluded from meeting this objective if you do not order or create any of the required information, except for “Patient name” and “Provider name” and office contact information.</td>
</tr>
<tr>
<td>You can also be excluded if your practice is in an area with low broadband availability.</td>
</tr>
<tr>
<td>For more information about qualifying for this exclusion, visit the <a href="http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/Stage2_EPCore_7_PatientElectronicAccess.pdf">Stage 2 Meaningful Use Specification Sheet</a> for this objective.</td>
</tr>
</tbody>
</table>
Compliance

Program Structure
Risk Identification
Work Plan
Get Started
Keep Going
Questions

Mary Hayes Finch, JD, MBA
334.271.7068
mfinch@alphca.com

Sharon Parker
sparker@alphca.com

Celeste Drayden
cdrayden@alphca.com