UW Health Compliance Committee

January 18, 2024, 5:00 - 6:30 PM

Via WebEx: https://uwhealth.webex.com/uwhealth/j.php?
MTID=mab9224abc457b1768fcd1367d76e9253

Meeting Number: 2634 697 9617 // Password: 011824

Join by phone +1-415-655-0003 US TOLL // Access code: 2634 697 9617

**ADVANCE MEETING MATERIALS ARE POSTED FOR REFERENCE. OCCASIONALLY, THE
POSTED MATERIALS DO NOT REFLECT CHANGES MADE SHORTLY BEFORE OR DURING
COMMITTEE MEETINGS. THE FULL COMMITTEE MINUTES ARE THE OFFICIAL RECORD OF
FINAL COMMITTEE ACTION**
<table>
<thead>
<tr>
<th>Time</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5:00 PM</td>
<td>I. Call to Order and Chair Announcement</td>
<td>Regent Mike Jones</td>
</tr>
<tr>
<td></td>
<td>UW Health Compliance Committee 2024 Meeting Schedule</td>
<td>FYI Attachment - UW Health Compliance Committee 2024 Meeting Schedule (Please add dates and times to your calendars)</td>
</tr>
<tr>
<td>5:01 PM</td>
<td>II. Meeting Minutes - Open Session</td>
<td>Regent Mike Jones</td>
</tr>
<tr>
<td>5:02 PM</td>
<td>III. UW Health Corporate Compliance</td>
<td>Mr. Troy Lepien</td>
</tr>
<tr>
<td></td>
<td>Presentation - UW Health Corporate Compliance</td>
<td></td>
</tr>
<tr>
<td>5:27 PM</td>
<td>IV. Closed Session</td>
<td>Motion to enter into closed session pursuant to Wisconsin Statutes sections 19.85(1)(e) and 146.38, for the discussion of confidential strategic matters that for competitive reasons require a closed session and for the review and evaluation of health care services, including but not limited to: review and approval of closed session minutes, discussions and overviews of compliance matters including corporate compliance, reimbursement compliance, research billing compliance, pharmacy compliance and privacy compliance; and pursuant to Wisconsin Statutes section 19.85(1)(g) to confer with legal counsel regarding action these and other matters.</td>
</tr>
<tr>
<td>6:30 PM</td>
<td>V. Adjourn</td>
<td></td>
</tr>
</tbody>
</table>
Attachment

UW Health Compliance Committee
2024 Meeting Schedule
UW HEALTH COMPLIANCE COMMITTEE

2024 MEETING SCHEDULE
(Via WebEx)
3rd Thursday of the months listed below:

January 18, 2024, 5:00 - 6:30 PM
   February - No Meeting
   March – No Meeting
April 18, 2024, 5:00 - 6:30 PM
   May - No Meeting
   June – No Meeting
July 18, 2024, 5:00 - 6:30 PM
   August – No Meeting
   September – No Meeting
October 17, 2024, 5:00 - 6:30 PM
   November – No Meeting
   December – No Meeting
Compliance Committee – Administrative Items

- Announcements – Schedule
- October Minutes
- Article of Interest – General Compliance Program Guidance November 2023
Compliance Committee – Administrative Items

- Office of Inspector General Guidance
  - 1998 First Compliance Program Guidance (CPG)
  - 2023 General Compliance Program Guidance (GCPGs)
    - Review key Federal authorities
    - Seven elements of a compliance program
    - Adaptations for small and large entities
    - Updating as needed
    - No longer publishing in the Federal Register
  - 2024 Industry Segment-Specific Compliance Program Guidance (ICPGs)
    - Tailored to Fraud & Abuse for each industry subsector
    - Updating as needed
  - Goal of the documents guide the development and evaluation of compliance programs
Corporate Compliance – Administrative Items

- Federal Laws
  - Federal Anti-Kickback Statute (AKS)
    - Prohibits entities involved in Federal health care program business from offering or receiving gifts to reward past or future referrals
    - Intent-based, criminal statute that prohibits remuneration, whether monetary, in-kind, or in other forms, in exchange for referrals of Federal health care program business
  - Physician Referral Law (i.e., Stark)
    - Prohibits a physician from making referrals for certain designated health services (e.g., lab, therapy, radiology, etc.) payable by Medicare to an entity with which the physician (or an immediate family member) has a financial relationship, unless an exception applies, and its requirements are satisfied.
    - Strict liability statute which is in effect regardless of intent or mental state when committing the action
Corporate Compliance – Administrative Items

- Federal Laws
  - False Claims Act
    - A way for the Government to recover money when an entity knowingly submits or causes to be submitted false or fraudulent claims for payment
    - Filing false claims may result in liability of up to three times the programs loss plus an additional penalty per claim filed (Each instance of an item or a service billed to Medicare or Medicaid counts as a claim)
    - Contains a whistleblower provision that allows a private individual to file a lawsuit on behalf of the United States and, if appropriate, entitles that whistleblower to a percentage of any recoveries
    - False Claims Act cases are pursued by DOJ on behalf of HHS in Federal court
Corporate Compliance – Administrative Items

- Federal Laws
  - Civil Monetary Penalty Authorities
    - Civil Monetary Penalties Laws
      - Addresses a wide variety of improper conduct related to Federal health care programs principally fraudulent and abusive conduct.
      - OIG can pursue assessments in lieu of damages, CMPs, and exclusion from participation in the Federal health care programs.
      - CMP cases are administrative and pursued by OIG before an HHS administrative law judge
      - Works in conjunction with False Claims Act
    - Beneficiary Inducements
      - Addresses any person who offers or transfers remuneration to a Medicare or State health care program that the person knows or should know is likely to influence the beneficiary’s selection of a service for payment
  - Information Blocking
    - Prohibits providers from engaging in practices that are likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information
Corporate Compliance – Administrative Items

- Federal Laws
  - Exclusion Authorities
    - OIG has the legal authority to exclude individuals and entities from participation in all Federal health care programs
    - Mandatory Exclusions – Patient abuse or neglect and felony convictions
    - Permissive Exclusions – Wide range of options from misdemeanors regarding health care fraud to engaging in arrangements that violate the Federal laws
  - Criminal Health Care Fraud Statue
    - Prohibits knowingly and willfully executing, or attempting to execute, a scheme to either:
      - Defraud any health care benefit program; or
      - To obtain, by means of false or fraudulent pretenses, representations, or promises, any money or property from any health care benefit program
    - The Government must prove beyond a reasonable doubt and prove that the defendant acted with intent to defraud, specific intent to violate this statute is not required for a conviction
Corporate Compliance – Administrative Items

- Federal Laws
  - HIPAA Privacy & Security Rules including HITECH
    - Addresses the use and disclosure of individuals' identifiable health information by covered entities to conduct certain health care transactions electronically
    - Requires appropriate safeguards to protect the privacy of information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization
    - Gives individuals rights over their information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections
    - Specify a series of administrative, physical, and technical safeguards for covered entities and their business associates to ensure, among other provisions, the confidentiality, integrity, and security of electronic PHI
    - Covered entities and their business associates can consider their organization and capabilities, as well as costs, in designing their security plans and procedures to comply with Security Rule requirements - NIST and the OCR Security Risk Assessment were noted as assessment tools
    - Requires covered entities and their business associates to provide notification following a breach of unsecured PHI
    - With increasing numbers of cybersecurity attacks aimed at HIPAA regulated entities of all sizes, compliance with Privacy, Security, and Breach Notification Rule requirements should be a top compliance priority and included in all risk assessments.
Compliance Program Infrastructure

- Written Policies and Procedures – Element 1 of 7
  - Provide a roadmap of duties/roles/oversight, workflows, documentation requirements, and implements entity-wide controls to mitigate compliance risks
  - Code of Conduct articulates the entity’s commitment to comply with all Federal and State laws and regulations - Tip: Signed message from CEO and signed endorsement by the Board
- Compliance Policies and Procedures
  - At least two areas:
    - (1) the implementation and operation of the entity’s compliance program, including the seven elements discussed in this section; and
    - (2) processes to reduce risks caused by noncompliance with Federal and State laws
  - The Compliance Committee should ensure that policy process fosters rather than undermines compliance culture
  - Policy and procedure on the screening of employees, contractors, etc. against exclusion lists
  - Developed under the direction and supervision of the compliance officer & Compliance Committee
  - Available to all relevant individuals within the organization
  - Compliance with the code and applicable policies and procedures should be part of the performance evaluations of all employees and contractors
  - Compliance Policies should be reviewed on an annual basis
  - Method to contact Compliance Officer with any questions
Compliance Program Infrastructure

- Compliance Leadership & Oversight – Element 2 of 7
  - Compliance Officer
    - Report either to the CEO with direct and independent access to the board or to the board directly
      - Sufficient stature within the entity to interact as an equal of other senior leaders of the entity
      - “Senior leadership” means the group of leaders who report directly to the executive leading the entity
      - Compliance officer should not lead or report to the entity’s legal or financial functions and should not provide legal or financial advice or supervise anyone who does
      - Compliance officers with the dual role of privacy officer should have sufficient staff and resources
    - Sufficient funding, resources, and staff to operate a compliance program capable of identifying, preventing, mitigating, and remediating the entity’s compliance risks
    - A large organization likely needs a department of compliance personnel with a variety of skills/expertise
  - Duties
    - Overseeing and monitoring the implementation and operation of the compliance program;
    - Advising the CEO, board, and other senior leaders on compliance risks facing the entity
    - Chairing the Compliance Committee;
    - Reporting to the board
    - Screening of employees & contractors
    - Independently investigating compliance matters
Compliance Program Infrastructure

- Compliance Leadership & Oversight – Element 2 of 7 (cont.)
  - Compliance Committee
    - Purpose is to aid and support the compliance officer in implementing, operating, and monitoring the Compliance Program
    - The Compliance Officer should be the chair of the Compliance Committee.
    - The Compliance Committee should be comprised of the relevant leaders of both operational and supporting departments and members have authority to speak for their department.
  - Duties
    - Analyzing the legal and regulatory requirements
    - Assessing, developing, and regularly reviewing policies and procedures
    - Monitoring and recommending internal systems and controls
    - Assessing education and training needs and effectiveness, and regularly reviewing required training
    - Developing a disclosure program and promoting compliance reporting
    - Assessing effectiveness of the disclosure program and other reporting mechanisms
    - Conducting annual risk assessments
    - Develop and evaluate the compliance workplan
    - Evaluating the effectiveness of the compliance program
    - Reporting periodically to the board assessing the Compliance Committee’s performance
Compliance Program Infrastructure – Element 2 of 7 (cont.)

- Board Compliance Oversight
  - The United States Sentencing Commission’s Guidelines require that an entity’s “governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.”
  - Corporate boards also have a fiduciary duty of care, which requires that boards assure that “information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information to allow management and the board, each within its scope, to reach informed judgments concerning ... the corporation’s compliance with the law . . . .” In re Caremark, 698 A.2d 959, 970 (Del. Ch. 1996)
  - Boards should consider creating a separate Board Compliance Committee with a charter to oversee health care compliance
  - Responsibility includes overseeing the compliance officer and the Compliance Committee
  - Assure that the compliance officer’s stature is equal with other entity senior leaders
  - Ensure that the compliance officer has sufficient power, independence, and resources to implement, maintain, and monitor the entity’s compliance program
  - The board should meet with the compliance officer on a regular basis and no less than quarterly
  - Regular executive sessions creates a continuous expectation of open dialogue
Compliance Program Infrastructure

- Training & Education – Element 3 of 7
  - The compliance officer should develop an annual training plan that includes the training topics by target audience
  - The Compliance Committee should review the training plan at least annually
  - All board members, officers, employees, contractors, and medical staff should receive targeted training at least annually
  - Potential Topics:
    - Identity and role of the compliance officer
    - Role of the Compliance Committee
    - Open communication with the compliance officer including ways to raise questions and concerns
    - Nonretaliation for disclosing or raising compliance concerns
    - Availability of training materials in different languages
    - Participation should be a condition of continued employment with consequences, up to and including possible termination for non-compliance
Compliance Program Infrastructure

- Compliance Program Infrastructure – Element 4 of 7
  - Effective Lines of Communication with the Compliance Officer & Disclosure Programs
    - An open line of communication between the compliance officer and entity personnel
    - Entity personnel should be informed about the ways they can reach the compliance officer directly (e.g., via email, telephone, messaging)
    - Should develop several independent reporting paths for an employee to directly report violations that cannot be diverted by supervisors or other personnel
    - At least one reporting path that permits individuals to report concerns anonymously
    - Posted in commonly frequented physical and virtual spaces
    - All disclosures of compliance concerns, including potential violations of entity policies or Federal or State requirements, should be recorded in a log maintained by the compliance officer or their designee
    - The compliance officer should include information about concerns and investigations in communications with the Compliance Committee, CEO and BOD
Compliance Program Infrastructure

- Enforcement Standards: Consequences & Incentives – Element 5 of 7
  - Consequences should be appropriate to the circumstances and intent (e.g., ignorance, negligence, or reckless conduct). Intentional or reckless noncompliance should subject individuals to significant sanctions.
  - The procedures should identify: the various consequences that may be imposed under specific circumstances involving noncompliance and the functions
  - The compliance officer should monitor investigations and resulting discipline to ensure consistency
  - All levels of employees should be subject to the same consequences for similar offenses
  - Excellent compliance performance or significant contributions to the compliance program could be the basis for additional compensation, significant recognition, or other, smaller forms of encouragement
  - The Compliance Committee should ask whether certain goals may inadvertently encourage risky or noncompliant behavior
Compliance Program Infrastructure

- Risk Assessment, Auditing, and Monitoring – Element 6 of 7
  - A formal compliance risk assessment process should pull information about risks from a variety of external and internal sources, evaluate and prioritize them, and then decide which risks to address and how to address them.
  - The Compliance Committee should be responsible for conducting and implementing the compliance risk assessment. With this information, the Compliance Committee can work with the compliance officer to prioritize resources and develop the compliance work plan, including audits and monitoring of identified risks based on priority.
  - Between compliance risk assessments, the compliance officer should continue to scan for unidentified or new risks.
  - The Compliance Committee should include in the compliance work plan a schedule of audits to be conducted based on risks identified by the annual risk assessment.
  - Any claims reviews and audits should include a review of the medical necessity of the item or service by an appropriately credentialed clinician.
  - Periodic assessments of the compliance program’s effectiveness.
Compliance Program Infrastructure

- Responding to Detected Offenses & Developing Corrective Action Initiatives – Element 7 of 7
  - Processes and resources to thoroughly investigate compliance concerns of violations of Federal or State law, and other types of misconduct
  - Compliance officer must act promptly to notify appropriate leaders and coordinate with entity counsel
  - Material violation of applicable law must be determined on a case-by-case basis. Monetary loss to a Federal health care program is not sole determinate
  - Record of the investigation should be maintained and contain:
    - Documentation of the alleged violation
    - Description of the investigative process
    - Copies of interview notes and key document
    - Log of the witnesses interviewed, and the documents reviewed
    - Results of the investigation and any disciplinary action or corrective action
  - If credible evidence of misconduct the compliance officer or counsel the entity should promptly (not more than 60 days after the determination) notify the appropriate Government authority of the misconduct
  - Prompt corrective action, including:
    - Refunding of overpayments - within 60 days after identification
    - Enforcing disciplinary policies and procedures; and
    - Making any policy or procedure changes necessary to prevent a recurrence of the misconduct.
Compliance Program Infrastructure

- Other Considerations
  - Quality & Patient Safety
    - OIG and DOJ have long emphasized the importance of quality and patient safety
    - OIG and DOJ have investigated and settled cases based on the submission of false claims for care that is materially substandard, resulting in death or severe harm to patients
    - OIG has entered into CIAs focused on quality of care and patient safety
    - Entities should incorporate quality and patient safety oversight into their compliance programs
    - Besides patient harm, quality and patient safety concerns, such as excessive services and medically unnecessary services, can lead to overpayments and may cause False Claims Act liability
    - The compliance officer should be responsible for implementing a compliance program that includes and addresses quality and patient safety compliance risks just as they do for any other compliance risk area integral to the entity’s health care segment
    - When conducting risk assessments, Compliance Committees should ensure that medical necessity, patient safety, and other quality compliance issues are included in the risk universe.