GBMC

Annual Compliance Training

False Claims Act

- A law dating back to the Civil War that prohibits one from presenting any claim for payment to the Government for an item or service that the person knew or should have known was false or fraudulent, or for medical services that were not medically necessary.
  - For example, if an entity submits a bill to Medicare for services that were not actually rendered; or
  - Routine waivers of co-payments or deductibles that are advertised as an inducement to patients.
- Each bill or submission for payment is a “false claim.”
- False claims will not be paid; civil penalties range between $5,500 and $11,000 for each false claim, plus treble the amount of damages sustained by the Government as a result of the false claims.
- Liability applies to people who know or should know the claim is false.

Example of a false claim:

1) Submitting a claim for an appendicitis instead of a stomach ache.

2) A provider uses the copy and paste feature in Epic to update a record; however details that need to be updated (e.g., side of body, amount of time, and persisting information like “drainage needed”), are not updated. So, the medical record for different patients and/or different encounters are identical and potentially incorrect. This also increases quality concerns.

Anti-Kickback Law

- A federal law with criminal and civil penalties that prohibits a person or entity from:
  - Knowingly and willfully (requires intent)
  - Directly or indirectly offering, paying, soliciting, or receiving
  - Remuneration
  - In order to induce or reward the referral or purchase of items or services to be paid for by federal healthcare benefit program (applies to everyone)

Examples of kickbacks include:

- Free trips and/or training in exchange for endorsing or prescribing drugs or devices;
- Offering to lease space or provide services at less than fair market value to physician who send a lot of patients to a hospital; and
- Lavish vacations, gifts, and annual “consulting fees” to endorse products, drugs or services.

Physician Self Referral (Stark Law)

- Prohibits:
  - A physician (only applies to physicians)
  - From making a referral
  - Of a Medicare or Medicaid patient
  - To an entity that furnishes “Designated Health Services”
  - If the Physician has a financial relationship with the entity
  - Unless an exception applies.
- This law can be enforced even if the person did not intend the result.

Examples of a violation of Stark:

- An orthopedic physician refers patients to a radiology practice in which s/he has an ownership interest.
- Hospital provides free use of its employees or free use of hospital space only to a high referring physician.
- Hospital provides higher call coverage payments to physicians who send more patients to the hospital, than to others in that specialty on call.

Stark and Anti-Kickback: Exceptions and Safe Harbors

There are exceptions and safe harbors to these laws, which include:

- Bona Fide Employment;
- Personal Services Contracts or Lease Agreements that are:
  - In writing and signed by both parties
  - For a term of at least one year
  - For a payment that is set in advance and that does not vary with the volume or value of referrals, and
  - Payment must be for fair market value

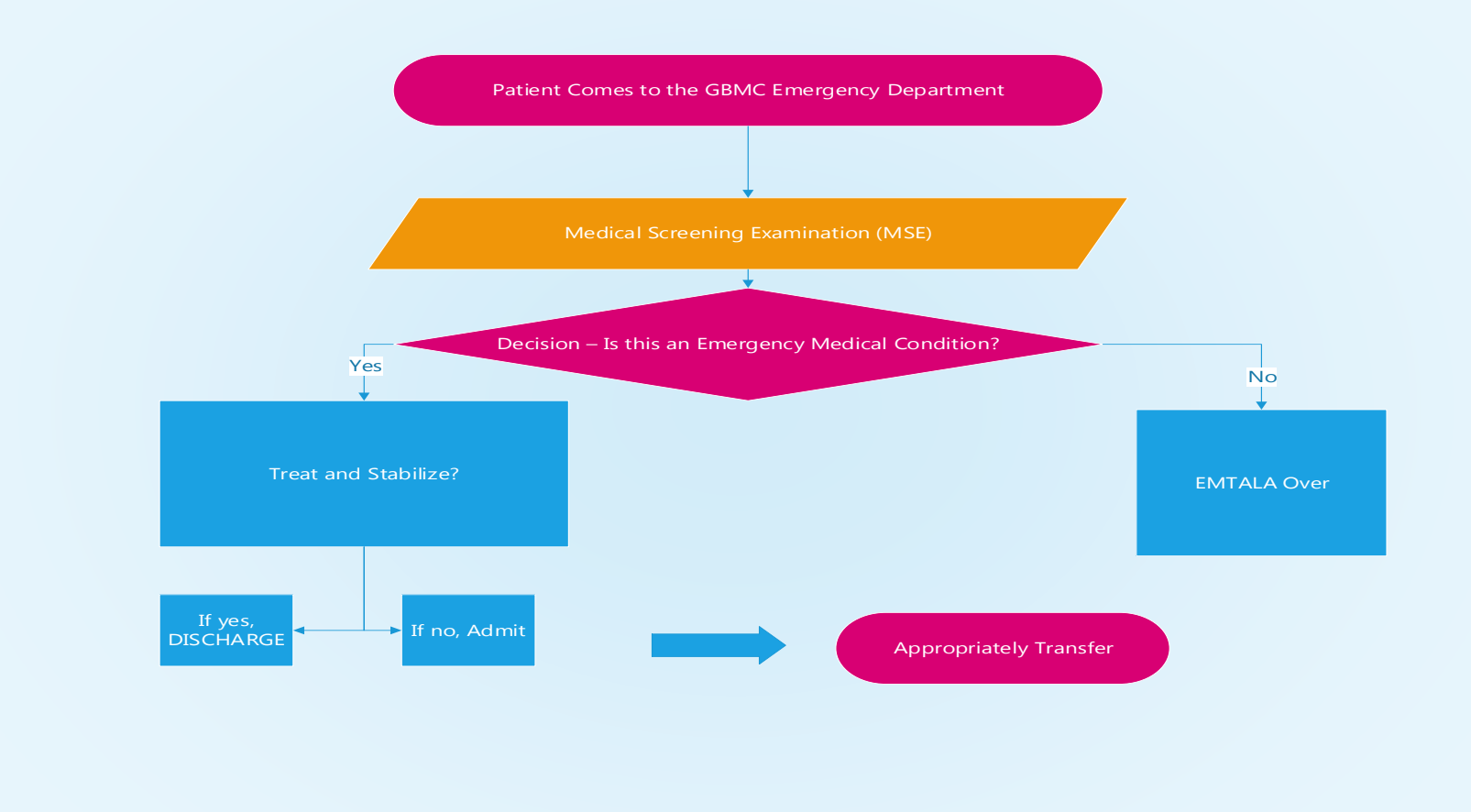
If a relationship involves payment of money to a physician or company that sends patients to or does business with the health care system, the legal and compliance departments must be involved to make sure the transaction does not violate these laws, or fits under an exception or safe harbor.

Exclusion Statute

- The Office of the Inspector General (OIG) MUST exclude providers and suppliers from participating in all Federal health care programs for certain activity, including but not limited to:
  - Medicare or Medicaid fraud;
  - patient abuse or neglect;
  - felony convictions for other health care-related fraud, theft, or other financial misconduct; and
  - felony convictions for unlawful manufacturer, distribution, prescription or dispensing of controlled substances
- Examples that MAY cause the OIG to exclude an individual or entity from Federal health care programs:
  - misdemeanor convictions related to health care fraud;
  - fraud in a program (other than a health care program) funded by any Federal, State, or local government agency
  - providing unnecessary or substandard services;
  - submitting false or fraudulent claims;
  - engaging in unlawful kickback arrangements; and
  - defaulting on health education loans or scholarship obligations
- *The effect of being excluded is that no Federal health care program payment may be made for any items or services furnished by an excluded person or at the medical direction or on the prescription of an excluded person.*

Social Security Act

- Medicare and Medicaid Programs
- Children's Health Insurance Program (CHIP)
- Emergency Medical Treatment and Labor Act (EMTALA)
  - EMTALA Flowchart:



United States Criminal Code

- Title 18 – Crimes and Criminal Procedure, section 1347
- Knowingly and willfully executing or attempting to execute a scheme to:
  - Defraud any health care benefit program; or
  - Obtain by means of false or fraudulent pretenses, representation, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program,
  - In connection with the delivery of or payment for health care benefits, items or services.
  - May result in a fine and/or imprisonment
  - If bodily injury occurs to the patient, such as when an unneeded medical procedure is performed, the penalty can be a prison term of up to twenty (20) years.

Example: Providing cancer treatments to patients that do not have cancer, resulting in bodily injury to the patients.

HIPAA

- Permitted uses of protected health information (PHI) include treatment, payment, and healthcare operations, e.g., credentialing and audits.
- Without a permitted use, the patient must provide a documented authorization in accordance with Maryland law.
- The “minimum necessary” standard requires that we disclose only the minimum information necessary to perform the task; the minimum necessary standard does not apply to treatment.
- When the Privacy Officer identifies a breach, GBMC is required to notify the patient and the Department of Health and Human Services. Government agencies can audit for compliance with privacy laws, which potentially results in fines and penalties.
- We are required to provide The Notice of Privacy Practices (NOPP) to all patients; this document explains the patient’s privacy rights.
- GBMC’s NOPP is at this link: http://infoweb/Workfiles/FORMS%20Notice%20of%20Privacy%20Practices_100117.pdf
- GBMC is required to have Business Associate Agreements. These contracts inform vendors that they must comply with the HIPAA Privacy and Security Regulations as well as GBMC’s requirements for handling our patient’s PHI.

HIPAA

- These are the data elements that identify patients under HIPAA:
  - name,
  - date of birth,
  - fax number,
  - account number,
  - web universal resource locator (URL),
  - street address,
  - electronic mail address,
  - certificate/license number,
  - license plate number,
  - city,
  - discharge date,
  - social security number,
  - vehicle and serial number,
  - device identifier and serial number,
  - precinct date of death,
  - medical record number,
  - internet protocol number,
  - full face photographic images,
  - zip code,
  - telephone number,
  - health plan beneficiary number,
  - biometric identifiers (i.e., finger prints),
  - any other unique identifying number, characteristic, or code (e.g., a unique tattoo)

Examples of HIPAA violations:

- Looking at a patient's medical record without a GBMC business related purpose.
- Faxing medical record information to an unintended recipient.
- Discussing patient care including PHI in public places.
- Failure to provide the Notice of Privacy Practices to patients.
- Failure to request the patient to acknowledge in writing that they received the Notice of Privacy Practices.
- Failure to have a Business Associate Agreement in place when protected health information is being shared.

Appropriate Use Agreement

- All employees and contractors are required to read and sign this agreement upon employment and as part of the annual competencies
- It defines Confidential Information as a collection of specific information including PHI
- The link to the Agreement is here: http://infoweb/workfiles/compliance/AppropriateUseAgreementRvsd_08152017.pdf
- Highlights:
  - Employees will not disclose any Confidential Information with other others, including friends, spouse, and family, unless in an authorized capacity and in the necessary scope of employment.
  - Employees will not discuss Confidential Information in public or common areas.
  - Employees will verify information to make sure it is given to the correct patient.
  - Employees will not look at their own medical record; they will use MyChart.
  - Employees will properly log out of computers and systems when not in use.
  - Employees will not look at medical records of other employees unless required in the capacity of their work and in the necessary scope of employment.

GBMC Code of Business Ethics

- The purpose of the Code is to articulate GBMC's message of fair competition and ethical business practices. It addresses some of the complex legal and business ethical issues we face every day and provides guidance for handling some specific compliance scenarios.
- Link to the GBMC Code of Business Ethics: http://infoweb/workfiles/Compliance/Code_of_Business_Ethics_revised_9.26.16.pdf
- Guiding Principles:
  - We strive to provide outstanding service to our patients.
  - We strive to abide by the law and maintain high ethical standards in our business decision making.
  - We strive to maintain a high standard of accuracy and completeness in our records.
  - We strive to maintain a professional and safe work environment.
  - We take personal responsibility for protecting the organization's resources and achieving our ethical goals.
  - We report our compliance concerns by using the appropriate chain of command.

Confidentiality of Information Agreement

- All employees and contractors are required to read and sign this agreement upon employment and as part of the annual competencies
- It defines Confidential Information as protected health information, personnel information, business operations information, and computer information and access.
- The link to the Confidentiality of Information Agreement is here: http://infoweb/body.cfm?id=536
- Highlights:
  - Violation of this agreement subjects the employee/contractor to disciplinary action up to and including termination or revocation of employment privileges by GBMC.
  - Unauthorized disclosure of legally protected information may result in civil liability or criminal prosecution.

Resources

- Anyone who has a suspected compliance issue is encouraged to discuss it with:
  - Their supervisor
  - The Chief Compliance Officer at 443-849-4327
  - The Compliance Hotline at 1-800-299-7991 (allows for anonymous reporting)
  - Email the Compliance Mailbox at Compliance@gbmc.org
  - Email the HIPAA Mailbox at HIPAA@gbmc.org