Corporate Compliance & HIPAA
New Associate Training
All new Methodist Le Bonheur Healthcare (MLH) Associates must complete this compliance training. It includes information to help you understand and comply with MLH Compliance Program and HIPAA Privacy and Security Policies and Procedures, the MLH Standards of Conduct, and the MLH Corporate Compliance Program.

Your actions ensure that Methodist Le Bonheur Healthcare is an organization of high integrity and ethics, and compliant with laws and regulations. In our daily work at MLH, we encounter compliance related activities and must make the right decision to do the right thing and to act appropriately.
What is Compliance?

- Compliance is knowing and following federal, state and local laws, regulations and guidelines that apply to your job.

- Methodist Le Bonheur Healthcare (MLH) is committed to conducting business activities in compliance with laws and regulations, MLH policies and procedures, the MLH Standards of Conduct, and the HIPAA Handbook.

- Compliance is the responsibility of all MLH Associates.

- As an Associate, you will be responsible for knowing and understanding the laws and regulations and MLH policies and procedures that apply to your job, and how to report suspected compliance violations.
The MLH Corporate Compliance Program Policy includes 7 elements of an effective compliance program as defined by the U.S. Federal Sentencing Guidelines:

1. Written Policies & Procedures and MLH Standards of Conduct
2. A Designated Compliance Officer and Compliance Committee
3. Training and Education
4. Effective Open Lines of Communication
5. Internal Auditing and Monitoring
6. Enforcement of Standards and Disciplinary Guidelines
7. Investigations and Corrective Action Plans
The MLH Corporate Compliance Department

**MLH Chief Compliance Officer, Privacy Officer**
Loretta Hinton
901-516-0567
Loretta.Hinton@mlh.org

**Director, Corporate Compliance**
Linda Maners
901-516-0735
Linda.Maners@mlh.org

**Privacy Auditor**
Kim Baltz
901-516-0868
Kim.Baltz@mlh.org

The **MLH Corporate Compliance Department** is located at:
1211 Union Avenue, Suite 700
Memphis, TN 38104
Fax: 901-516-0569
How Do I Comply With the MLH Compliance Program?

Responsibilities of New Associates

• Read and comply with:
  - The *MLH Standards of Conduct*,
  - The *HIPAA Handbook*,
  - MLH Policies and Procedures (available on the MLH Intranet website “MOLLI”.)

• Understand and comply with laws specific to your job.

• Attend staff meetings and training programs.

• When you are not sure, ask for help from your supervisor or the Corporate Compliance Department.

Do the right thing and act appropriately.
You are responsible for reporting compliance violations. Report issues to:

- Your Supervisor/Leader
- The Compliance Hotline 1-888-220-2163
- The Compliance Department 901-516-0735
- The Corporate Compliance Department website - “Submit a Question” link.

Write to:
Methodist Le Bonheur Healthcare
Corporate Compliance Department
1211 Union Avenue, Suite 700
Memphis, TN 38104
What Compliance Issues Should I Report to the Corporate Compliance Department?

Suspected issues or violations an Associate may report include:

- HIPAA Privacy or Security (HIPAA Breach)
- Insurance Fraud
- Fraud and Abuse with Billing Medical Claims
- Identity Theft
- Coding and Billing Irregularities
- Inappropriate Gifts or Entertainment from Vendors
- Kickback & Bribes
- Auditing Matters
- Questionable Accounting or Internal Auditing Controls
- Provider Credentials
- Copyright Laws
Where Can I Find Corporate Compliance Information?

- Corporate Compliance Website on MOLLI – the MLH Intranet website.

- *MLH Standards of Conduct* – provides guidance to our Associates to help you understand the legal and ethical obligations of your job.

- *MLH HIPAA Handbook*

- Compliance Newsletter
HIPAA (Health Insurance Portability and Accountability Act) is a federal law (Privacy & Security) that makes –

- **Healthcare Organizations** (e.g., hospitals, physician offices, clinics, home health agencies, etc.)
- **Healthcare Providers** (e.g., doctors, nurses)
- **Healthcare Plans**

...protect the privacy of their patients and all the information about them by safeguarding **Protected Health Information ("PHI")**.

**Privacy Rule:** Protects the privacy of individually identifiable health information.

**Security Rule:** Sets national standards for the security of electronic PHI (ePHI).

**Breach Notification Rule:** Requires Covered Entities (CEs) and Business Associates (BAs) to provide notification following a breach of unsecured PHI.
The **Privacy Rule** sets the standards for how confidential or **Protected Health Information (PHI)** – verbal, written and electronic format should be protected from unauthorized use.

**Protected Health Information or “PHI”**
- “PHI” is one type of confidential information.
- Information about a patient’s health that **identifies** him/her in any way.
- Related to a person’s condition, treatment, or payment.

**Examples of “PHI”:**
- Medical Records (e.g., diagnosis, treatment, allergies, medical history and physical, etc.)
- Medications or Prescriptions
- Oral Communications about a Patient’s Health
- Test Results (e.g., X-ray, MRI, lab)
- Billing or Claims Information
- Information tied to a patient’s health that identifies the patient in any way.
Protected Health Information ("PHI")

Examples of PHI that could be tied to information about
a person’s health, include:

- Name
- Geographical Subdivisions Smaller than State – Street Address, City, County, Zip Code
- Date of Birth/Death; Age
- Telephone Number
- Fax Number
- Email Address
- Social Security Number
- Medical Record Number
- Credit Card Number
- License Number
- Vehicle License Plate
- Fingerprint
- Full or Partial Face or Other Identifiable Images, even X-ray
- Unique Identifying Characteristics.
MLH HIPAA Officers

Privacy Officer

Loretta M. Hinton
Chief Compliance Officer

Methodist Le Bonheur Healthcare
Corporate Compliance Department
1211 Union Avenue, Suite 700
Memphis, TN 38104
901-516-0567
Email: Loretta.Hinton@mlh.org

Call the Privacy Officer with questions about privacy of verbal, paper or electronic patient information and to report HIPAA violations.

Information Security Officer

Steve Crocker
Chief Information Security Officer

Methodist Le Bonheur Healthcare
Information Technology Services
5865 Shelby Oaks Circle
Memphis, TN 38134
901-516-0360
Email: Steve.Crocker@mlh.org

Call the Information Security Officer with questions about security of electronic patient information and protection of our computer systems.
Review of HIPAA Policies and Procedures

- Only look at patient information when you are directly involved in the patient’s care or your job requires that you “Need to Know” the information.

- The MLH HIPAA policies are located on MOLLI under “Forms & Policies”.

- Keep patient information private.

YOU are responsible for protecting PHI!
Notice of Privacy Practices for Protected Health Information Policy

Health Systems use a Notice of Privacy Practices to tell patients about HIPAA at check-in on the first visit, including:

- Common Uses and Disclosures (meaning to give out) of the patient’s information.
- Patient Rights
- How a patient can file a Privacy Complaint.

The Notice of Privacy Practices –

- Is posted at MLH (i.e., lobby, waiting room) and on our website.
- May be provided in paper copy or emailed to an individual if requested.
- Patients should sign an acknowledgement form for receiving the NOPP.

**PATIENT RIGHTS:** Under HIPAA, patients have the right to:

- Review and get a **copy of medical and billing records** – electronically if available.
- Make a **written request** for an **accounting of disclosures** (a list of who MLH gave the patient’s information to) of PHI made outside our Health System and Medical Staff. Refer to MLH policy – Accounting of Disclosures.
ACCESSING PATIENT INFORMATION

As healthcare providers, you are assigned access to patient information in paper and electronic medical records to do your job.

You may only access or disclose (meaning to give out) PHI for treatment, payment or healthcare operations, or with a signed authorization by the patient giving permission to release his/her confidential information.

You may NOT view a patient record or information, or give out information for any other reason (e.g., curiosity, because someone asks you to look, etc.)

NO SNOOPING!
HIPAA Privacy Rule Allows Uses and Disclosures of PHI For the Following Purposes

**Treatment of Patients**
- Provide, coordinate or manage health services.
- Consults between providers.

**Payment of Patient Claims/Bills**
- Bill claims
- Obtain payment for providing care to a patient.
- Obtain pre-authorization for services.

**Health Care Operations of the Health System and Its Medical Staff**
- Audits
- Training
- Quality Improvement
- General Business of the Health System

Refer to MLH Policy – *Use and Disclosures of Protected Health Information for Treatment, Payment or Healthcare Operations.*
When using, disclosing, or requesting PHI or patient information, you should limit the information to the “Minimum Necessary” (meaning least amount of information needed) for its medically intended purpose to complete a task or your job.

Only use or disclose PHI on a NEED TO KNOW BASIS!

An example includes:

- **If a request is made for a radiology report, only give out that report and not the entire medical record.**

The Minimum Necessary Rule does not apply to uses and disclosures for treatment, made to the patient, or made prior to the patient written authorization.

Additional information requires a signed authorization by the patient before PHI may be released to outside parties such as a marketing firm or life insurance.

Refer to MLH policy – **Minimum Necessary Disclosure and Determination** on MOLLI.
Use and Disclosure of Protected Health Information to an MLH Patient or Patient’s Personal/Legal Representative

Personal or Legal Representative
A person (e.g., parent, family member, legal guardian) with legal authority to make healthcare decisions on behalf of the individual or minor child.

Partners in Care (PIC)
- May be a family member or friend.
- Chosen by the patient and are part of the communication team. For example, they may receive information about the patient’s medical status and discharge plan.
- Information may be shared for the patient’s present hospitalization.
- Does not replace a patient’s legal representative if one is listed.
- The patient should be asked at every date of service who the patient wishes to identify as the Partner in Care.
Uses and Disclosures for PHI to Family Members, Close Friends, or Others Involved in the Care of the Patient

A patient should be asked who (family, friend, personal representative) MLH may share his or her PHI with for patient care, payment and notification purposes.

The patient should be given the chance to agree or to prohibit or restrict the use or disclosure of PHI, and this should be documented.

Privacy Safeguard –

• When providing paper information (i.e., discharge instructions, lab work) to a patient or personal representative, make sure every page is for that particular patient.
• Make sure another patient’s information is not mixed in. For example, when the department uses a shared printer to print out patient information, look at every page to make sure it all belongs to that patient.
• Always verify you are giving, mailing, faxing the correct records to the patient, personal representative or provider.
Patients have a right to request to restrict (meaning to limit release of certain patient information) the use and disclosure of their PHI. Examples:

- A patient asks that his diagnosis not be shared with his family members or visitors.
- A patient asks in writing not to give his PHI to his health insurance plan when he pays in full out-of-pocket for the health care item or service. By law we may be required to comply with the request.

**DO NOT** view a medical record that is not part of your job responsibility.

- If a family member asks you to look at their record (such as to view a lab result), the family member/patient or personal representative must first sign an authorization form and place it on file with the facility Health Information Management (HIM) Department or Medical Records.
- If you look without signed authorization on file, you may violate MLH policy and HIPAA, that may result in corrective action.
According to the Office for Civil Rights – *Communicating with A Patient’s Family, Friends, or Others Involved in the Patient’s Care*, examples are presented when a provider can share PHI:

• A surgeon who did emergency surgery on a patient may tell the patient’s spouse about the patient’s condition while the patient is unconscious.

• A hospital may discuss a patient’s bill with her adult son calling with questions about charges to his mother’s account.

But:

• A nurse may **NOT** tell a patient’s friend about a past medical problem unrelated to the patient’s current condition.

• A provider is not required by HIPAA to share a patient’s information when the patient is incapacitated or not present, and can choose to wait until the patient has an opportunity to agree to the disclosure.
Incidental Use or Disclosure occurs when PHI is accidentally seen or overheard during appropriate uses or disclosures of information in the healthcare setting.

Example: A patient overhears a physician speaking to a patient in another room in the Emergency Department.

Incidental uses or disclosures are allowed if:
• We reveal only the minimum necessary information, and
• We have in place proper administrative, physical, and technical safeguards (as required by HIPAA).

Protect PHI as if it were your own!
Physical Safeguards

Verify that your work environment has reasonable physical, technical and administrative safeguards:

• **DO NOT** talk about patient issues with friends, family or in public areas (i.e., cafeteria or elevators). Be aware of your surroundings.

• Speak in a low voice when discussing patient information in patient care or interview areas so others can’t easily hear.

• Use a curtain or privacy screen to block the view or close the room door to provide privacy.

• Secure areas with patient information to keep it safe from unauthorized individuals.
  - Lock doors or file cabinets.
  - Limit visitors to restricted areas.

• **DO NOT** leave file room or file cabinet keys out in the open.
Breach Notification

A “Breach” is when unsecured PHI is accidentally or wrongfully used or disclosed.

Examples of Potential Breaches:

- Lost or stolen unencrypted laptop with PHI.
- Failing to shred patient files before throwing them in the trash.
- Leaving medical records in plain view.
- Sending emails or faxes with PHI to the wrong address/number.
- Giving a patient another patient’s records or discharge papers accidentally.
- Posting patient information on social media.
- Gossiping or looking in medical records of friends, relatives, co-workers, high profile persons or others.

NO SNOOPING!

Report HIPAA violations to your supervisor, the Privacy Officer, or the Corporate Compliance Department. The Privacy Officer will decide if a violation is a breach, and if it must be reported by law to the patient, media and federal government within 60 days of the breach.
Sale of PHI or Use or Disclosure of PHI for Personal Gain

- IS PROHIBITED!
- IS ILLEGAL!
- SHOULD NOT BE DONE!

Examples:
- Selling or using a patient list to promote a product.
- Removing patient lists when you leave the hospital/medical office practice.
- Using the hospital patient lists to promote your or someone else’s personally owned business.

Ask the Privacy Officer for exceptions.

REMEMBER: If you are ever contacted and asked to give out or sell patient information, immediately report this to the Corporate Compliance or Legal Department.
Use and Disclosures of PHI in the Facility Directory

Facility Directory
A listing of individuals in a healthcare facility. May include:

- Name
- Location in the facility (i.e., hospital)
- Condition in general terms (“Good” or “Fair”). Do not give specific medical information about the individual.
- Religious affiliation may only be given to members of the clergy.

At arrival, ask the patient if he/she want to be listed in the facility directory.

If a patient requests “no publicity” or not to be posted in the facility directory:

- **DO NOT** disclose that the patient is present in the facility (i.e., hospital).
- For example, you may tell a caller/visitor, “We do not have a patient by that name listed in our facility directory.”

If a patient agrees to being listed in the facility directory, then a caller may be informed of the patient’s location or room number.
Confidentiality and the Release of Patient and Associate Information

• All patient and Associate employment information is confidential (meaning intended to be kept private).
• DO NOT DISCUSS or RELEASE this information except when needed to do your job or to provide patient care.
• Original patient medical records are the property of the hospital. Unauthorized removal of records from MLH is grounds for corrective action.

*If you see PHI lying around (i.e., patient list, lab slip, OR schedule), pick it up and make sure that it is delivered to the appropriate person/place or contact the Corporate Compliance Department at 901-516-0735.
Amendment of Protected Health Information

• Patients have the right to request amendment of medical records. For example, a patient believes PHI in her health record is incomplete or incorrect, and requests an amendment (or change) of the information.

• Amendment requests must be made and responded to in writing.

• Requests for simple corrections to demographic or billing information may be accepted verbally.

• Contact the facility HIM or Medical Records Department for Amendment requests.

• Refer to MLH Policy – Amendment of Protected Health Information.
Social Media

Because you work in the health care industry, you are constantly exposed to confidential, highly sensitive patient and business information.

**DO NOT USE OR DISCLOSE** patient or confidential business information on social media sites.

**STOP and THINK** before you post on social media.

You are responsible for your online content and posts. Even the best of intentions can violate MLH social media and privacy policies. Social Media includes: Facebook, Snapchat, YouTube, Twitter, Instagram, LinkedIn, Pinterest, Google Plus+, etc.
DO NOT POST THE NAME OR INFORMATION OF A PATIENT.

NEVER discuss a patient or their care or post photos of patients or co-workers without their permission.

Examples of Prohibited Posts
✓ I had a terrible day. 22 year old patient died in ED.
✓ I love my new job. I got to treat a burn victim today!!
✓ Can you believe it? My patient named her baby ..... 

Never ridicule or discuss patients or their families in a disrespectful manner even if in jest.

The Patient Posted It First
Be cautious. It is OK for the patient to disclose his or her own personal health information. It is safer if you don’t share or retweet it on your personal accounts.

It is NOT Private
What you say is public and will be public for a long time. DO NOT say anything on Facebook or other sites that you would not say in a public area where others have access to the information.
SOCIAL MEDIA

“Like” a Post

- Do Not “Like” a post that includes patient information or a photograph, or makes fun of a patient or co-worker. You are endorsing the post.

For additional information on social media, refer to the MLH Associate Handbook.

Report inappropriate social media posting to the Corporate Compliance Department or the Human Resources Department.

Violations of social media restrictions may result in disciplinary actions particularly if it results in a privacy violation.
• **ENCRYPT AND PASSWORD PROTECT** your laptop or other portable device and portable media (i.e., CDs, USB drives, DVDs) with PHI or CBI saved on it.

• Because of their portability (meaning small size and easy to move), laptops, cell phones and other portable devices are at risk of theft and must be kept secure from unauthorized individuals.

• If you do not know if your laptop is encrypted, contact Information Systems to install hard drive encryption software.
Laptop, Portable Device, Media and Offsite Use of ePHI and CBI

- Only persons with approved reason may store PHI or CBI on portable devices (i.e., laptop, cell phone) or media (i.e., USB drives).

- **DO NOT** allow others to view PHI or CBI on a laptop screen.

- Keep laptop and other devices and media safe and within sight when in public or traveling.

- Log out or shut down laptop when unattended.

- **DO NOT LEAVE A LAPTOP UNATTENDED IN A VEHICLE.**
  If necessary, lock it or other portable devices or media securely in the trunk.

- **NEVER LEAVE A LAPTOP IN A CAR OVERNIGHT.**

- When not in use, keep in secure areas, such as a locked drawer, cabinet or a locked office.
Remote Access to PHI and CBI

Remote Access – Looking at MLH information from home, off campus, out-of-town, or through a device not directly connected to the MLH Network.

Remote Access:
- Must be approved by a Senior Leader.
- Ask Information Technology for questions how to protect the data and for technical compatibility.
- For the Internet, use routers/firewalls on home networks.
- **Encryption must be used** on routers/firewalls that use wireless technologies.
- Avoid printing information offsite. If you must print, protect and keep the information confidential, and dispose of it properly, such as shredding.
Faxing Associate Employment and Patient Information

- Always use a Cover Sheet with contact information and a confidentiality statement.
- Fax to secure locations.
- Place fax machines in secure locations not open to the public.
- Confirm and type in the correct fax number before hitting the “send” button.
- Check for receipt of the fax (e.g., call to see if received, fax confirmation sheet).
- Complete an Information Security/Privacy Variance Report for misdirected faxes.
- Ask that misdirected faxes be returned to MLH (e.g., mail or other), if that is not possible, ask the receiver to shred the fax.
Systems and applications with PHI and CBI require a unique user ID and password.

**Password Control**  
**KEEP PASSWORDS CONFIDENTIAL.**

**DO NOT SHARE** your password with others!

Passwords should be at least 8 characters minimum, with at least one capital letter, one numeral, and one special character.

**Protect it at all times** – if you think your password has been compromised, you should contact the IS Help Desk immediately at 901-516-0000, or Physicians Help Desk at 901-516-3111.
Beware of Phishing Emails

Do not click on a suspicious email that may be a phishing email such as the one below. A fraudster may send a phishing email to payroll trying to steal money by posing as the Associate asking to change the direct deposit banking information for their paycheck.

From: Nancy Smith
To: Payroll, HRIS
Subject: [EXTERNAL] Direct Deposit info Update

Payroll’s Name,
I changed my bank and I’d like to change my paycheck dd details, can the change be effective for the current pay date?

Below is the banking information:
Bank Name: GO BANK
Routing # 111111111
Account # 222222222

Regards,
Nancy

TIPS TO IDENTIFY PHISHING EMAIL: Identify where the email came from – internal or external flagged warning in the subject line as [EXTERNAL]. Follow policy and procedure to change direct deposit information.
Measures to Secure Emailed PHI

- **ENCRYPT** outgoing email that contains PHI.
- To encrypt, type the word “encrypt” in the subject line of the email. (Email sent internally can not be secured through this system.)
- Encryption puts the email into an unreadable code to ensure that unauthorized people cannot read the email and use the PHI to steal someone’s identity to cause them harm.
- Always check email before hitting “send.”
- **NEVER** send PHI to your personal or private email address, even if you encrypt it as you send it out.
Cell Phone – Photographs and Video

- **DO NOT** take photos of patients with personal cell phones.

- **NEVER** photograph or video patients with cameras, cellular phones, smart phones, or similar devices.

- All photographs of patients become part of the medical record and the property of MLH.

- All facilities have an official camera/equipment to use for patient care purposes. An example is photographs to track a skin rash or wound.

- Contact the Legal Department for consents and authorization forms for video recording or photographing patients.

- Do not text patient information.
HIPAA Auditing

• The Corporate Compliance Department conducts routine audits and investigational audits (when a patient or other person suspects someone may have accessed their electronic medical record) on users (e.g., Associates, Physicians) accessing MLH electronic medical records.

• Access of electronic records must be part of the user’s job responsibility for treatment, payment, or healthcare operations, or with a signed authorization on file at the facility or in the medical record.

➢ DO NOT share your computer user name or password with anyone. REMEMBER: Your user name and password tie any computer activity to you! We audit for security compliance.

➢ Our system creates a snapshot of the records you view, print, forward and disclose. We can tell if you are viewing or sending PHI, when you should not. COMPLY WITH HIPAA!
IDENTITY THEFT PREVENTION

IDENTITY THEFT
Your personal information (e.g., name, SSN) is used, without your permission, to commit fraud or other crimes (e.g., a credit card or an account is opened in your name).

MEDICAL IDENTITY THEFT
An Identity Thief uses your name or health insurance to get medical care or services (e.g., see a doctor, get prescription drugs, file claims with your insurance plan).

To Prevent Identity Theft/Medical Identity Theft:
• Ask patient for an ID to verify identity.
• Protect & secure patient and business information.
• Do not leave information in public areas, on fax or copy machines, or viewable on computer screens.
• Mail letters with PHI or CBI in post office collection boxes or at the Post Office, not in unsecured mailboxes.
• Shred paper with PHI or patient information in designated security containers.
• DO NOT put PHI in regular trash cans where it can be stolen.
• Encrypt devices with PHI - laptops, cellphones, and removable media – USB drives, CDs.
• Refer to MLH policy – Identity Theft Prevention Policy.
IDENTITY THEFT PREVENTION

Notify the Corporate Compliance Department if you think that identity theft/medical identity theft has happened.

Examples include:

- A patient reports getting a bill for services that he did not receive, and thinks that someone has used his identity.
- The patient does not look like the photo or description on an ID.
- Information given does not match what is on file (e.g., SSN, date of birth).
- Family or friends call the patient by a different name.
- The medical record has different health information (e.g., different blood type) or procedures.
CODING & BILLING ACCURATE CLAIMS

One of the largest risk areas for hospitals is filing claims for payment from Federal Healthcare Programs, such as Medicare and Medicaid/TennCare.

- Patient records should be accurate and complete.
- Document accurately and timely. Good documentation helps ensure quality patient care.
- Bill only for services that are provided and documented correctly.
- Correct any billing errors and repay money received in error within 60 days of finding the error.
- When paid too much, repay the money within 60 days of finding the overpayment.

False Claims Act – a law that makes it illegal to file a false claim with the government (Medicare or Medicaid/TennCare).
DO NOT COMMIT FRAUD

DO NOT commit fraud, even if you think your intentions are good.

Fraud is illegal!
Government Investigations
If someone contacts you at work or at home about your work and says they are from the government, you should:
• Contact the Corporate Compliance Department 901-516-0735.
• Send any document or letter that they give you to the Legal Department – Fax: 901-516-0569.
• Ask for identification and a business card to identify where they work.
• Do not destroy documents or try to hide evidence.

Government agencies include:
• Office of Inspector General (OIG)
• Centers for Medicare & Medicaid Services (CMS)
• Department of Health and Human Services (HHS), Office for Civil Rights (OCR)
• Federal Bureau of Investigation (FBI)
• Tennessee Bureau of Investigation (TBI)
ETHICAL GUIDELINES FOR ASSOCIATES INTERACTING WITH VENDORS

Vendors or Sales Representatives market and/or sell products and services to MLH (supply, equipment, instrument, pharmaceutical or medical device.)

Associates may **not** accept the following from Vendors:

- Gifts, including cash, entertainment, gifts baskets, trips.
- Pre-printed prescription pads, pens, post-it notes, and other advertising items.
- Meals/Food (e.g., business lunch, free meal at a free vendor sponsored programs “After Hours”, or food provided at a meeting or inservice at MLH.)

**Why all the worry about vendors?**

Our patients should feel convinced that the products and services we buy from vendors for the patient’s care are based on quality and cost-efficiency, not on what gifts or events the vendor can offer to the provider or Associate.
Methodist is allowed by Tennessee law to have one raffle per year as an approved fundraising event.

The Methodist Healthcare Foundation conducts this annual event with Board Approval and Tennessee Secretary of State application approval.

At Methodist, we may not have other raffles, cakewalks or games of chance. These are illegal.

Report any raffles, cakewalks or games that involve money in exchange for a prize to the Corporate Compliance Department.
The Emergency Medical Treatment and Labor Act (EMTALA) is a federal law that applies if a person comes to the Emergency Department or other hospital area and asks for an exam or treatment of an emergency medical condition, the hospital must provide an appropriate Medical Screening Exam (MSE) to decide if an Emergency Medical Condition (EMC) exists.

**DO NOT:**

- Delay or deny emergency treatment to the patient.
- Give the patient/family member directions to another facility, even if asked.
- Tell the patient/family that the wait is long or give wait times.
- Tell the patient that we don’t provide a service. For example, telling a pregnant patient that University Hospital does not have OB services. This could be seen as pressuring or coercing the patient to go to another facility.
- Delay the Medical Screening Exam (MSE) or stabilizing treatment to ask the patient about insurance or payment.
EMTALA applies for patients anywhere on the main Hospital campus, including area owned by MLH within 250 yards of the main buildings, including parking lots, sidewalks, driveways, and hospital departments.

If emergency assistance may be needed for a patient on MLH property, call the hospital operator and give the location of the person.

The operator will follow the facility Emergency Response Plan [that may require calling an adult or pediatric code (Dr. Emory House or Harvey Team) or calling 911].

If the Code Team or 911 is not required, ask the operator or available healthcare providers in the area for help, and transfer the patient to the hospital Emergency Department (ED).

Remain with the person until a physician, paramedic, the Code Team or other health care professionals arrive to help.
Sanctioning of Associates

- **Sanction** means when a person does not comply with a law, rule, or policy that leads to a penalty or corrective action being imposed.
- Violations of a severe nature may result in reporting to law enforcement officials, regulatory, accreditation, and/or licensure boards.

**Penalties or Consequences for Violating the Law**
- Corrective action up to termination.
- Required to refund payment received from health care plans and patients.
- You can personally face criminal prosecution – fines, penalties and prison.
- Fines and other penalties:
  - **False Claims Act** – For filing a false claim, you can be fined up to 3 times the program’s loss, plus **$11,463 to $22,927** per claim.
  - **HIPAA** – Penalty **$100 to $50,000** per violation up to **$1.5 million**, and up to 10 years in prison.
  - **Civil Monetary Penalties Law** – For abusive conduct, including filing a false claim, penalties are **$20,000 to $100,000** per violation.
Prohibiting Retaliation Against Associates, Individuals, or Others

• MLH will not allow retaliatory action (meaning to payback in kind; revenge; threaten; discriminate) against any Associate or individual who reports problems or concerns.
• It is the responsibility of MLH Associates to report perceived misconduct, including violations of laws, regulations, policies & procedures, or the MLH Standards of Conduct.
• MLH promotes an “Open-Door” policy at all levels of management to encourage Associates to report problems and concerns.
• Associates are encouraged to report concerns or suspected violations to leaders, and to ask questions when they are not sure about a process, policy, or other.
• Associates who commit or condone retaliation against an Associate for reporting an issue or assisting in an investigation will be subject to discipline, up to termination.
• Refer to the MLH policy – Prohibiting Retaliation Against Associates, Individuals, or Others
Doing What is Right

Working for an organization of high integrity makes us proud. Sometimes making the right decision for compliance can be difficult or confusing. If you are unsure, ask yourself a few simple questions:

- Is this the right thing to do?
- Are my actions legal?
- Does it comply with our Standards, MLH policies, and laws?
- Is this in the best interest of MLH and the patients we serve?
- Am I being fair, honest, and truthful?

The **MLH Standards of Conduct** guides you on what actions and behaviors are expected and considered appropriate. If you are in doubt or have questions, contact your supervisor, the Legal Department, Human Resources Department, or the Corporate Compliance Department.

Service    Integrity    Innovation

Quality    Teamwork