2016
Annual Associate Safety Modules

Section 12 Security

Methodist Le Bonheur Healthcare is Committed to Your Security and Safety

Be treated well.

Methodist Le Bonheur Healthcare

Your Personal Safety and Security

- on the street
- in the parking lot
- in your work area

Personnel Identification

- You must wear your ID badge at all times while on campus
- Badge must be worn above the waist, with picture visible at all times
- Do not place stickers or pins on your badge, unless MLH required (i.e. flu shot sticker)
- Contractors and vendors are required to have badges designated temporary

Personnel Identification

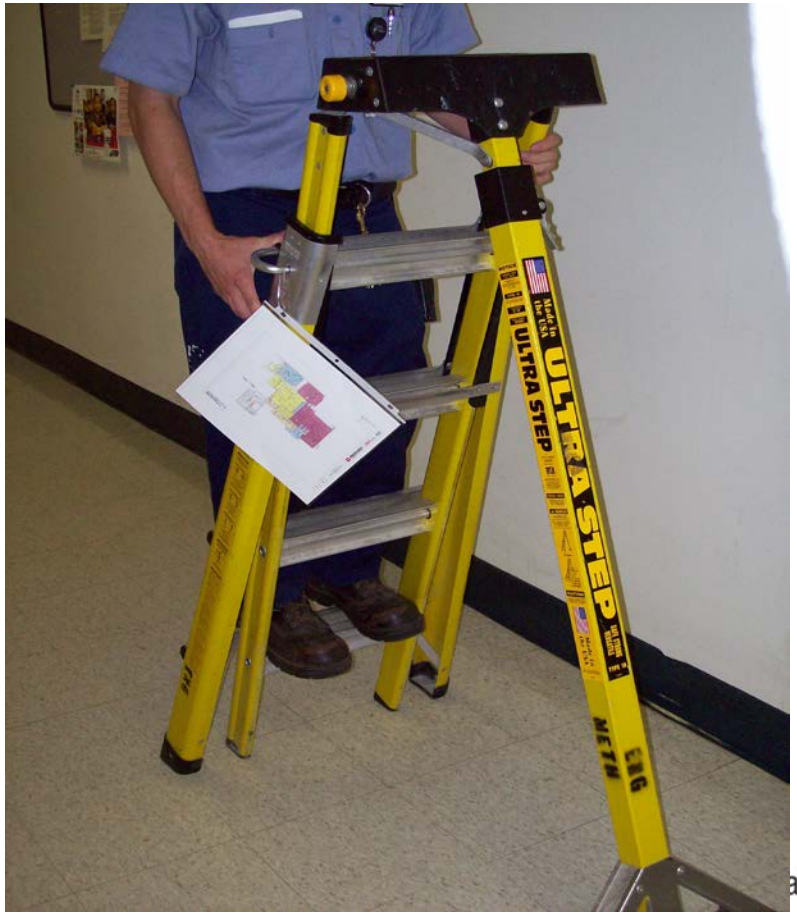
- If you loose your badge, report it to Security immediately and obtain a new badge
- ID badges are a good customer service tool, it allows patients and visitors to know with whom they are interacting.
- ID badges allow access into the facility after hours, into various departments within the facility, and into parking areas

Contractors Identification

- Contractors working in your area must have a badge
- If the contractor is working above ceiling, they must have a permit
- If the contractors do not have a badge and or a permit, call Facilities Services to let them know workers are in your area un-authorized

Contractor's Permit

- Permits will be hanging from the contractor's ladder



ated well.

Methodist Le Bonheur Healthcare

Walking To and From Your Car or Outside

Remember and follow these safety tips at all times

- Avoid walking alone. If you are unable to find others to walk with you, remember . . .
  - When walking, make a point of being aware of those around you
  - Always keep your head up and walk confidently
  - While still at a distance, survey the area underneath and around your vehicle
  - If you see someone suspicious do not approach your car, instead, notify security immediately

Walking To and From Your Car or Outside

- Be aware of vans parked next to your vehicle, and Enter your vehicle on the side farthest away from the van
- Always have your “destination key” in-hand before you reach your vehicle
- Do not talk on your cell phone

In Your Work Area

- How to reduce on-the-job security risks
- Elevator Safety
- Suspicious persons and activities
- Personal space and property

Elevator Safety

- Look before entering to make sure no one is hiding inside
- If a suspicious person is inside, then wait for another elevator
- Always stand near controls
- If your are attacked, push as many buttons as possible
- If a suspicious person enters you should get off
- If you are concerned about someone who is suspicious and waiting with you on an elevator, act as if you forget something and leave
- If elevator fails, use elevator phone to call for help

Always Be On the Alert

Make sure that everyone entering your work area is wearing the proper identification:

- ID Badge with visible picture
- Wrist Band (Patients)
- Contractor or vendor stickers

Always Be On the Alert

If you encounter anyone who is not wearing ID or appears out of place . . .

- Politely ask “May I help you.”
- If, after confronting them, you are still suspicious, call Security.

Always Be On the Alert

- If you are uncomfortable approaching a suspicious person, or if you see suspicious activity
  - Call Security
  - Observe the person or situation
  - Locate the person for Security
  - Describe what you saw

Protect Your Personal Property:

- Never leave your pocketbook, wallet, or valuables out in the open, and never carry large amounts of cash.

- Make sure all doors, windows, drawers, cabinets, etc. are locked if left unattended.

- Never leave your keys our ID badge in view.

Remember:

- Immediately report any suspicious persons or activities to Security
- In the event of any crime, do not disturb the crime scene, and call Security as soon as possible

Use of Portable Electronic Devices

- MLH maintains a cache of laptop and other devices for emergency/disaster use. It is important to remember that during emergency use, ePHI rules still apply.
- Electronic Devices include, MLH-issued laptops or other portable media and mobile devices (e.g., CDs, DVDs, and USB flash drives PDA's, cell phones).
- Reasonable precautions must be taken by users to ensure that access to any portable device is not available to unauthorized individuals.

Standards for User Responsibility

- Laptops will require a username and password to access the MLH network.
- Portable media containing PHI or CBI must be encrypted (e.g. CDs, USB drives, DVDs).
- Laptops and portable media should be kept under the control and within sight of the user when in public places. When traveling (e.g., airports, hotels), particular care and caution should be taken.
- Users are responsible for immediately reporting potential security breaches, the theft or loss of laptops or other MLH portable devices to their Leader, to Security for offense and police reports, and to the Corporate Compliance Department by completing an Information Security/Privacy Variance Report (ISVR).

Standards for User Responsibility

- Laptops should be logged out and turned off when unattended.
- Reasonable precautions must be taken to physically protect devices that contain or remotely access MLH information from access or use by unauthorized individuals. Information must not be left open to compromise during offsite use.
- Do not leave portable devices or media unattended in a vehicle. If it is necessary to leave the devices or media unattended in a vehicle for a short time, these should be locked securely in the trunk, out of sight. Never leave a laptop or portable media in a car overnight.

Standards for User Responsibility

- When not in use, laptops and portable media should be kept in secure areas, such as a locked drawer or cabinet or within a locked office.
- Laptop users should copy information to the MLH network (P: drive) frequently to reduce the risk of losing information should the hard drive fail or if the device is lost or stolen. Laptop users should connect to the MLH network at least every 30 days to ensure critical patches and virus updates are applied to the device.
- Printing information offsite should be avoided. But if it cannot be avoided, printed information will be safeguarded, kept confidential, and disposed of properly (i.e. shredded).