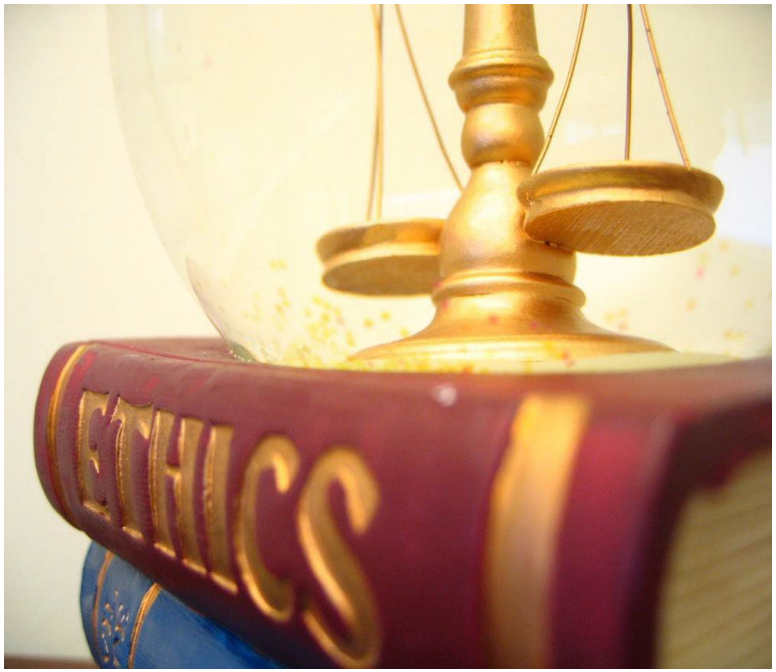
PRIVACY & COMPLIANCE

August 2022

Beth Israel Lahey Health
Lahey Hospital & Medical Center

Compliance = Doing the Right Thing

- **Compliance is…**
  - **Behaving ethically**
  - **Following the law**
- **Code of Conduct: *Integrity at Work***
  - List of ethical standards that *ALL* employees must follow
- **Culture of Compliance:** Federal government mandates compliance programs for health care organizations



Compliance Team

Lahey Hospital & Medical Center

Kelley McCue

- Director, Compliance and Privacy

Beth Israel Lahey Health System

Kaitlin McCarthy

- Associate Deputy Compliance Officer

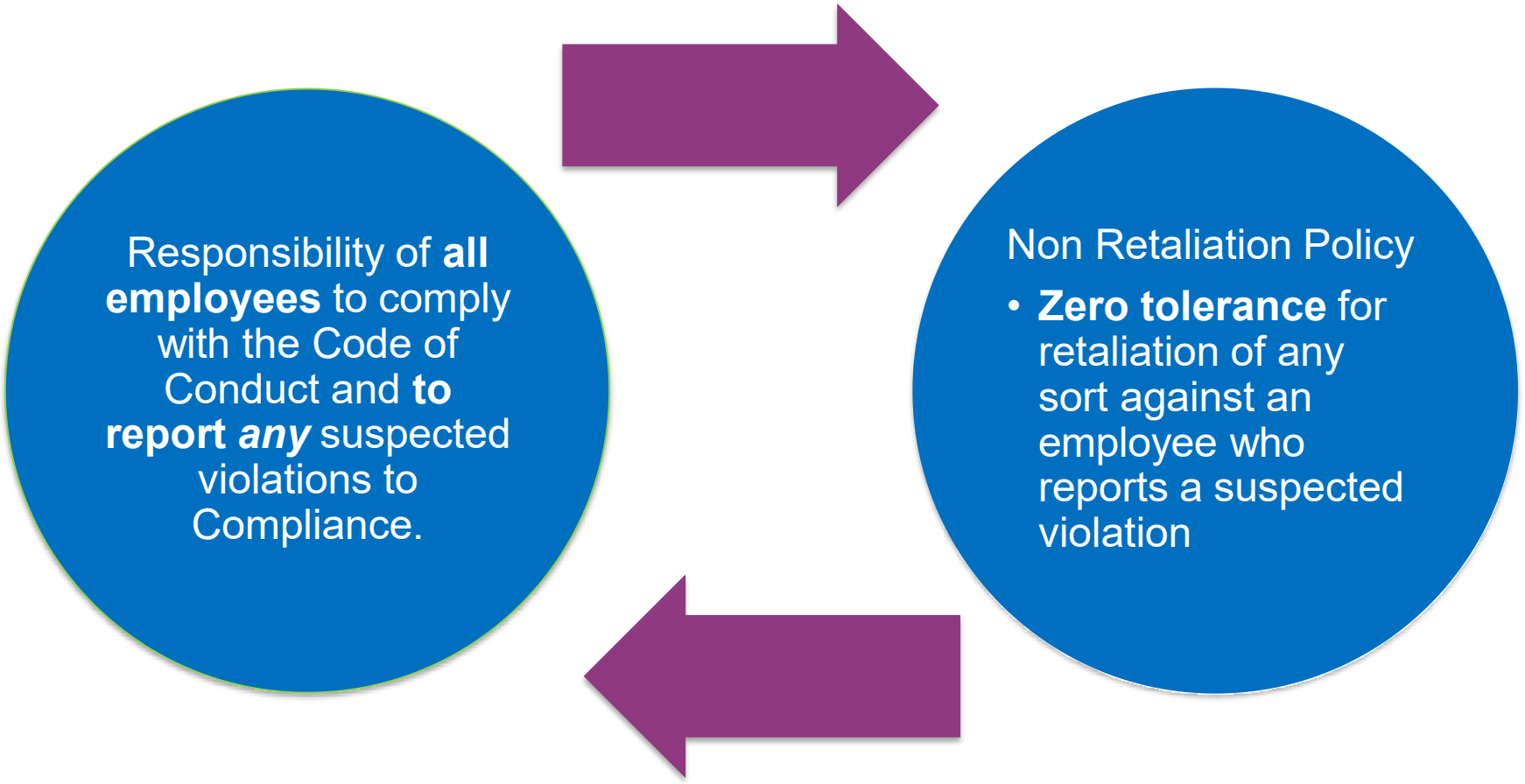
Lori Dutcher

- Chief Compliance Officer

… and the most important member…

YOU!!!

Speaking Up


Responsibility of **all employees** to comply with the Code of Conduct and **to report *any*** suspected violations to Compliance.
Non Retaliation Policy
• **Zero tolerance** for retaliation of any sort against an employee who reports a suspected violation

When To Speak Up?

Call Compliance immediately if…

You think an employee or vendor is doing something unethical, illegal or improper.

Ex. Stealing (work time, hospital resources, patient property)

You are not comfortable with action that you think may not be in the best interest of our patients.

Ex. Not providing an assistive device to a patient who needs one

You disagree with how a provider is billing for services.

Ex. Billing for care not provided

A patient voices concerns about a privacy issue.

Ex. Patient receives another patient's medical information in the mail

HIPAA

Goal: Protect the privacy and security of our patients' Protected Health Information (PHI).

Benefits of HIPAA compliance:

- **Patients trust and communicate openly with health care providers.**
- **Reduce risk of fines and harm to Lahey's reputation.**

HIPAA

PHI - Any information that relates to the past, present, or future healthcare of an individual ***and*** identifies that individual.

Includes: (but not limited to)

- Name
- Date of Service
- Email
- Phone #
- Medical / Clinical Information
- Photos
- Medical Record #
- Any other identifying code, number, picture, etc.

How do we promote HIPAA compliance?

Policies & Processes

Education & Training

Investigation, Auditing & Enforcement

HIPAA Policies:

- *Confidentiality of Patient Information*
  - Employees responsible for keeping secure and
  - confidential the information collected about our patients
- *Corrective Action Policy* – Details disciplinary process
  - Verbal counseling
  - Written warning
  - Termination

HIPAA Privacy Do's & Don'ts

DO:

- ✓ Ask yourself, "Do I need to know this to do my job?" before looking at protected health information.
- ✓ Close exam room doors when caring for patients or discussing their health concerns.
- ✓ Follow Lahey Hospital & Medical Center's policy for disposing of PHI and patient information – make sure to place all paper containing PHI in a Shred-It bin.
- ✓ Tell your supervisor / compliance if you see patient information in an open trash container.
- ✓ Turn computer screens so patients and other individuals can't see information on the screen.
- ✓ Double-check e-mail addresses and fax numbers before sending patient information.
- ✓ Request 2 identifiers (name & DOB) to verify a patient's identity before disclosing PHI.
- ✓ Report **ALL** privacy concerns to your supervisor or privacy officer including lost or stolen PHI.

HIPAA Privacy Do's & Don'ts

DON'T:

- ✗ Talk about patients in public places, such as elevators, hallways or cafeteria lines.
- ✗ Allow faxes or printed e-mails containing PHI to lie around the office.
- ✗ Leave Epic open while you leave the room to care for another patient.
- ✗ Keep materials that connect patients' names with their conditions out in the open where anyone can see them.
- ✗ Leave phone messages containing sensitive patient information on answering machines or voicemail systems.
- ✗ **Go into patient medical records unless you have a clinical or business need to do so.** (PROTENUS - inappropriate use audits)An access monitoring system is in place to monitor the appropriateness of all user access to the EHR.

IT Security Best Practices

- ***All*** Lahey Hospital & Medical Center colleagues have the responsibility to protect the organization's electronic information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

- Users are expected to follow security policies and exercise responsible, ethical behavior when using our computer network facilities, equipment, and applications.

- If you have questions please reach out to IT Security at ITSecurity@Lahey.org

IT Security Do's & Don'ts

DON'T:

- ✗ Share your computer account name or password with ***anyone***.
- ✗ Open email attachments or click on web links without first verifying the sender. These "phishing" attempts are a serious threat to our networks and resources.
- ✗ Dispose of electronic media that may contain ePHI into the normal trash. Call the IT Service Desk and ask Desktop Services to come take it away.
- ✗ Use email other than o365 for Lahey Hospital & Medical Center business.
- ✗ Use any unapproved data storage platforms for Lahey Hospital & Medical Center
- ✗ Do not leave your workstation or other devices unlocked when not in use.

IT Security Do's & Don'ts

DO:

- ✓ Report ***all*** computer viruses, suspicious activity, or lost/stolen devices to the IS Service Desk **immediately**.
- ✓ Encrypt ***all*** electronic PHI stored on any media.
  - ✓ Only approved encrypted USB drives can be used to store PHI.
  - ✓ Emails with PHI must also be encrypted: add **@encrypt** anywhere in the subject line to encrypt the email as well as its attachments.
- ✓ Only use approved software that is licensed for use by Lahey Hospital & Medical Center.
- ✓ Remember physical security: Never leave mobile devices or laptops in places where they are not secure.
- ✓ Go to IT Security page on MassNet or email ITSecurity@lahey.org with any questions.

Social Media

- Never post information, including photos and recordings, about patients, family members, visitors, or research subjects on social media.
- Do not talk about patients or research subjects, named or unnamed including “likes” and comments. Information you share could identify a patient even if a name or image is not shared.
- Never post a Lahey logo or confidential business information
- Some patients may give permission to Media Relations to post certain stories or personal information on BILH social media sites
- Always make clear that opinions are your own and not of your organization. Consider using a disclaimer such as “The postings on this site are my own and do not necessarily reflect the views of Lahey Hospital and Medical Center.

Gifts

- Colleagues may accept gifts of nominal value (such as a flower arrangement, holiday basket, baked good or the like) from patients or patients' family and visitors.
- Gifts of cash, cash equivalents or any item of other than a nominal monetary value is prohibited.
- Personal Gifts from vendors (including but not limited to food or beverage, calendars, pens, tickets to entertainment or sporting events, meals at restaurants except for education purposes, cash, or gift cards) are prohibited.
- Charitable donations can be directed to Philanthropy.

See the Policy on Acceptance and Solicitation of Gifts, Grants, Contributions and Donations for more information.

Conflict of Interest

- **What is a business conflict of interest?**
  Any situation in which you or a family member have a personal interest (including a financial interest) that may influence, or may reasonably appear to influence, how you carry out your job
- **Who may be involved?**
  You or a family member who is a spouse or domestic partner, child, parent, sibling, or any person living in the same household
- **What do I need to do?**
  Let your manager or leader know if this situation comes up; you may need to formally disclose your interest to the organization. Some colleagues may be required to complete a conflict of interest disclosure form.
- **What may happen?**
  You may need to remove yourself from some decisions.

Compliance/HIPAA Question?

- **Kelley McCue**
  BILH Integrity and Compliance
  AMC Director, Compliance and Privacy Officer, LHMC
  T: 781-744-9714
  E: Kelley.mccue@lahey.org

- **BILH Speak Up Hotline: 888-753-6533**
  Hotline Website: ***www.bilh.ethicspoint.com***

- **Compliance Intranet Site (MassNet)**

- ***Privacy@Lahey.org***

SPEAK UP – COMPLIANCE WILL BE THERE WHEN YOU DO!