Confidentiality and Corporate Compliance Training

Corporate Compliance Officer: **Lisa Ruddy**
Lapeer County Community Mental Health

This training will provide you:

- Information on Corporate Compliance
- Definition of PHI (Protected Health Information)
- Information on the requirement to report complaints and how to report complaints

Corporate Compliance is:

Lapeer County CMH's ability to comply with in the rules, regulations, guidelines, and policies created by the government, insurance programs and other funders. Corporate compliance is focused on Fraud, Waste and Abuse. Lapeer CMH and the provider network are responsible for accurate clinical documentation and accurate billing.

Corporate Compliance is:

More than a program within an organization, it is an organization-wide philosophy that guides decision-making.

What does it look like at the individual level?

- Following laws and rules that govern healthcare
- Being honest, responsible, and ethical
- Preventing, detecting, and reporting unethical and illegal conduct
- Preventing, detecting, and reporting Fraud, Waste, and Abuse (FWA) of Federal and/or State funds

Fraud, Waste, & Abuse

Fraud: An intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to himself or some other person. It includes any act that constitutes fraud under applicable Federal or State law.

Waste: Overutilization, underutilization or misuse of resources.

Abuse: Provider practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost to the Medicaid program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. It also includes beneficiary practices that result in unnecessary cost to the Medicaid program.

Fraud, Waste, & Abuse

Examples of fraudulent activity that must be reported:

- Billing for services not provided (False Claims-Fraud)
- Providing higher cost service than needed (Waste)
- Altering claim forms to receive more money (Fraud)
- Providing services that do not meet the recognized standard – example is staffing ratio (Abuse)
- Billing for non-covered services (False Claims-Fraud)
- Duplicate billing for a single service (Fraud)

Whistleblowers Protection

- State and Federal Laws to protect employees who report a violation or suspected violation (unless the employee knows the report is false)
- No retaliation and no discrimination in any manner against an employee by the employer for reporting
  - No discharge
  - No threats
  - No discrimination regarding compensation, terms, conditions, location, or privileges of employment
- Federal Law provides a reward in the form of a share of the recovery

Protected Health Information (PHI)

It is the responsibility of every employee to protect the privacy and security of sensitive information in **all** forms.

Printed

Spoken

Electronic

Protected Health Information (PHI)

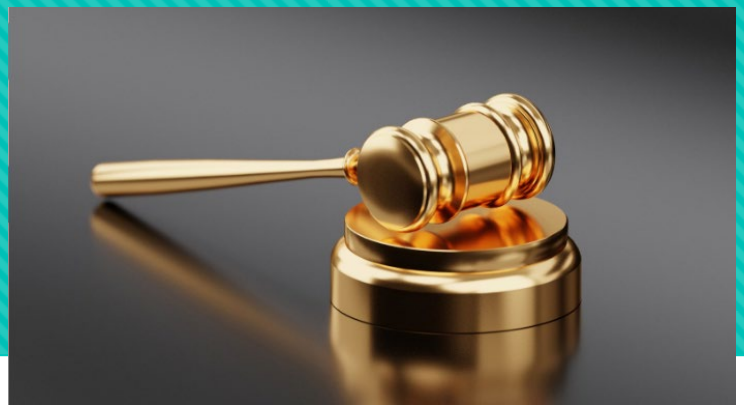
PHI is generally defined as any information that can be used to identify a person (whether living or deceased) that relates to the person's past, present, or future physical or mental health condition, including healthcare services provided and payment for those services.

Examples of PHI

When one of the following identifiers is combined with health information it creates PHI:

- Patient names/case numbers
- Address and telephone numbers
- Fax numbers
- Social Security Numbers
- Vehicle identifiers
- E-mail/web addresses
- Names of Relatives
- Health care record number
- Account numbers
- Fingerprints or voice prints
- Health plan beneficiary numbers
- Any other unique numbers or codes

Privacy Breach Penalties



Breaches of the HIPAA Privacy and Security Rules have serious ramifications for all involved. In addition to sanctions imposed by the agency, such breaches may result in civil and criminal penalties.

Statutory and regulatory penalties for breaches may include:

- Civil Penalties: $50,000 per incident up to $1.5 million per incident for violations that are not corrected, per calendar year
- Criminal Penalties: $50,000 to $250,000 in fines and up to 10 years in prison

Data Breach

- Cardiothoracic surgeon convicted of "snooping" in the Electronic Record of his co-workers, immediate supervisor and Hollywood celebrities, served 4 months in Federal Prison
- CVS and Rite Aid fined millions for disposing PHI in open dumpsters
- UCLA and Kaiser Hospital fined millions for failure to keep employees from "snooping" in Electronic Medical Records

Data Breach

- Massachusetts General Hospital fined one million dollars, because PHI was left on a subway

- An employee at Oakwood Hospital posted the following statement on her Facebook, "Came face-to-face with a cop killer and hoped he rotted in hell" The employee was emotional following the shooting death of a Taylor Police Officer. She worked for the hospital that treated the police officer AND the shooting suspect. The employee was fired.

Data Breach

- Most breaches, even those involving over 500 people, are caused by individuals, **not** system failures
- Be extremely cautious against loss and theft when dealing with electronic devices that store or have access to electronic PHI

Most Common Breaches

Privacy Breaches

- Theft
- Unauthorized Access
- Loss
- Hacking / IT Incident
- Improper Disposal
- Other

Security Breaches

- Laptop
- Paper records
- Portable electronic devices
- Desktop computer
- Network server
- Email
- Electronic health record

Typical Individual Violations

- "Malicious intent" – looking up someone's PHI when they have no business looking at it
- Discussing a person served with someone who has no need to know about their health information
- Using a personal cell phone to conduct business

Things to Remember

- Absolutely no conversations out in the public example: grocery stores
- Avoid conversations out in the open
- Avoid conversations in front of other residents

Electronic Equipment

- Position monitors so that they are not viewable by visitors, if possible
- Use privacy screen in high traffic areas
- Minimize displayed documents if someone approaches your desk
- **Do not** tell anyone your login or password

Electronic Equipment

- If applicable, do **not** leave your laptop in your car during a home visit or overnight
- Do **not** keep confidential information on a zip stick or disc
- There should be **no** confidential info saved to your desktop

Electronic Communication

- OASIS or the electronic medical record is the safest form of electronic communication
- All e-mails must contain the confidentiality statement
- When sending e-mails, always use initials or case ID's when e-mailing outside the agency
- A person served can request to communicate by e-mail
  - A release must be signed and no PHI should be sent

Electronic Communication

- Do **not** leave confidential papers on the fax and double check the fax number
- Be conscious of confidential conversations while on your cell phone
- If you take a picture of a consumer the picture must be left at the facility
  - Do **not** take pictures of consumers with your cell phone
- Do **not** put identifying information on your cell phone
- Texting - **no** PHI should be exchanged through texting

Social Media

- Don't be "friends" with a consumer
- If you are a "friend" of someone who is receiving services from you, you don't have to "unfriend" them – talk with Recipient Rights Officer, Supervisor or Compliance Officer
- Think through implications of "friending" a co-worker

Written Documentation

- Double check that confidential information is not accidentally thrown in the recycle bin instead of the shredder
- Use initials in your planner and do **not** leave it in your car
- Do not put any PHI (SSN, medical information, etc.) on a calendar in a public area

Written Documentation

Do not leave confidential papers or medical records:

- On the copier
- On your desk – lock them up
- In your car (even after a Med review or doctor's appointment)

Remember:

1. People from other homes / agencies don't necessarily have a "need to know" regarding consumer information

2. Access OASIS **ONLY** for your job responsibilities. OASIS date stamps **EVERY** access and documents that are printed

3. ALL STAFF must clearly understand that casual review for personal interest of patients' protected health information is unacceptable, against the law, and against the Policies and Procedures of Lapeer CMH

Reporting Complaints

LCCMH Corporate Compliance
Lisa Ruddy
810-245-8550

Region 10 Corporate Compliance
Kristen Potthoff
810-216-9434

Recipient Rights Officer
Lisa Jolly
810-667-0500

You must report complaints within 24 hours. If it is an abuse or neglect complaint it must be reported immediately.

Reporting Complaints

- You can stay anonymous!
- You can never be retaliated against for **good faith reporting** of compliance concerns or Recipient Rights Violations
- If you overheard something and are not sure if it has been reported, **report** it

Reporting Complaints

- Failure to report may result in disciplinary action up to and including termination
- All consumers will be notified if involved in a breach, even if the consumer hasn't made an inquiry
- Patients can file complaints with the HHS Office of Civil Rights however, they have no private rights to sue

How to File a Report with the State

MDHHS / Office of the Inspector General

1 (855) MI FRAUD (643-7283)
www.Michigan.gov/mdhhs

Michigan Department of Health & Human Services
Office of the Inspector General
P. O. Box 30062
Lansing, MI 48909

Questions?

Corporate Compliance
Lisa Ruddy
lruddy@lapeercmh.org
810-245-8550

Recipient Rights Officer
Lisa Jolly
ljolly@lapeercmh.org
810-667-0500