HIPAA Hints

- Protected Health Information (PHI) must be kept private!
- Use and disclose PHI for treatment, payment and operations as permitted by federal and state law
- Think about where you are and who can overhear you
- Think before you share PHI—written, verbal and electronic
- Use ### or click “send secure” button when emailing PHI
- Use the minimum amount of PHI necessary to get the job done
- Never share your password

Corporate Compliance Contact Information

Compliance Hotline
1-888-413-4313

Compliance Office
1-856-507-7857

compliance@ihn.org

No adverse action or retribution will be taken against any employee for reporting in good faith suspected non-compliance with federal and state laws, Code of Conduct, and internal policies and procedures.

Non-Retribution Policy

PATIENT PRIVACY IS EVERYONE’S RESPONSIBILITY
What is HIPAA?
• Health Insurance Portability and Accountability Act of 1996
• Protects the written, spoken and electronic forms of PHI

What is Protected Health Information (PHI)?
• Individually identifiable health information

What are examples of PHI?
• Name
• Address
• Dates (birth, discharge, admission, death)
• Phone and fax numbers
• Email addresses
• Social Security Numbers
• Medical Record Numbers
• Drivers license information/ Vehicle identifiers
• Account numbers
• Device numbers/Serial numbers
• Finger/Voice prints

HIPAA Hazards
• Snooping in medical records
• Unencrypted laptops and mobile devices
• Use of PHI on Social Media
• Posting or sharing photos and videos containing PHI
• Disclosure of sensitive medical information
• Improper disposal of PHI
• Releasing patient information without authorization
• Gossiping

Privacy Monitoring Program
Inpira protects electronic health records by monitoring for inappropriate or unusual accesses such as:

Coworkers/Managers
Family Members
VIPs
or
High Patient Access
Self Access
Self Modification
Other Suspicious Activities

******

Do not access records unless you are doing so within the scope of your job!