
Banner Health Information Security and Privacy Training Team

Morgan Raimo
Paul Lockwood

PHI Storage InfoGraphics

TO CLICK OR NOT TO CLICK: ACCEPTABLE USE POLICY

Always use Banner Health Wi-Fi, not Guest or public Wi-Fi

Never send protected health information (PHI) or other Non-Public Information via unsecure methods like external instant message, external email and text messages

Forwarding or sending Banner Health email to your personal email accounts is prohibited

ACCEPTABLE USE POLICY*

NEVER USE BANNER HEALTH DEVICES FOR PERSONAL USE
and
NEVER USE PERSONAL DEVICES FOR BANNER HEALTH USE

ANYTHING DONE ON THE BANNER HEALTH NETWORK IS SUBJECT TO REVIEW AND MONITORING

*Please refer to Banner Health Acceptable Use Policy. For more information, please contact InformationSecurity-PrivacyTraining@bannerhealth.com

ELECTRONIC MEDICAL RECORDS: PROTECTING PATIENT PRIVACY

CARE FOR OUR PATIENT DATA

TOP 3 CAUSES OF DATA BREACHES

EMPLOYEE ACTION

LOST OR STOLEN DEVICES

THIRD PARTY ERROR

UNDERSTAND THE POLICY**

YOU SHOULD NEVER ACCESS RECORDS FOR THE FOLLOWING:

- Yourself
- Friends & family
- Any patient not under your direct care

ACCESS RECORDS FOR YOUR DIRECT PATIENTS ONLY

Only disclose or request information that is absolutely necessary for you to do your job

Never use, disclose, or request sensitive medical records unless it is specifically justified

KNOW WHO MAY REQUEST RECORDS:

Legally authorized representatives

Patients

DO YOUR PART

- KNOW THE POLICIES
- DO NOT SHARE LOGIN/CREDENTIALS
- SECURE ACCESS
- REPORT VIOLATIONS TO YOUR SUPERVISOR
- FOLLOW THE BANNER NECESSARY USE POLICY

**Please refer to Banner Health Acceptable Use Policy. For more information, please contact InformationSecurity-PrivacyTraining@bannerhealth.com

LOCK IT UP: THUMB DRIVES & ENCRYPTION

SMALL DEVICE, BIG RISK

A thumb drive is a removable storage device, also known as a flash drive or memory stick

Thumb drives not approved by Banner Health will not work on company owned devices

To get an approved encrypted thumb drive, contact the Data Protection Team*

ALOST THUMB DRIVE CAN RESULT IN A \$150K FINE and CORRECTIVE ACTION**

ENCRYPTION EXPLAINED***

Encryption is a security practice used to code messages to protect unauthorized people from accessing the information

to encrypt an email

1. Create a new message in Outlook
2. Complete the message including subject, recipient, and attachments
3. Type "encrypt" in the body of the message before clicking send

Messages sent between Banner Health devices are automatically encrypted

Messages sent to a non-Banner Health email address are not automatically encrypted

DO YOUR PART

Only store necessary data on an approved encrypted thumb drive

Make sure you use a Banner Health approved encrypted thumb drive

If you accidentally used an unencrypted email or lost a thumb drive, please report it to your supervisor

*The Data Protection Team can be contacted at DataProtection@bannerhealth.com
**App Name: Database of Health Care Reports, October 21, 2016
***Banner Health's PHI is encrypted if transmitted between Protected Health Information and Patient Care Hub Data Policy

For more information, please contact InformationSecurity-PrivacyTraining@bannerhealth.com

TEXTING & UNSECURE EMAIL FORWARDING

DID YOU KNOW?

When you send an email it passes through different servers and computers before it reaches its intended recipient

Securing your email makes sure that only the intended recipient can access it via password and will help you avoid a security breach or HIPAA violation

External IPs are not secure, however Internal IPs are considered secure and HIPAA compliant

Your texts are not secure, even on a Banner Health issued phone

Not all business-related emails are secure, including any email you send or receive from an outside source

DO YOUR PART

DO NOT SEND SENSITIVE OR PATIENT INFORMATION VIA TEXT OR UNSECURE EMAIL

Never send sensitive patient or payment information via unsecure methods, such as text message, email, or paging systems

Do not forward Banner Health email to your personal email accounts or use personal accounts to conduct business; your other accounts are not secure

How do I make an email secure?

1. Create a new message in Outlook
2. Complete the message including subject, recipients, and attachments
3. Type "encrypt" in the body of the message before clicking send

For more information, please contact InformationSecurity-PrivacyTraining@bannerhealth.com



PHI Data Storage and Sharing

Cybersecurity and Privacy Training and Awareness



Table of Contents

- What is Protected Health Information (PHI)?
- Common PHI Violations
- PHI Exposure Risks
- What You Can Do
- Questions

What is Protected Health Information (PHI)?

PHI stands for Protected Health Information. Examples of PHI include:

Any information that identifies an individual and relates to their **past, present, or future medical condition**

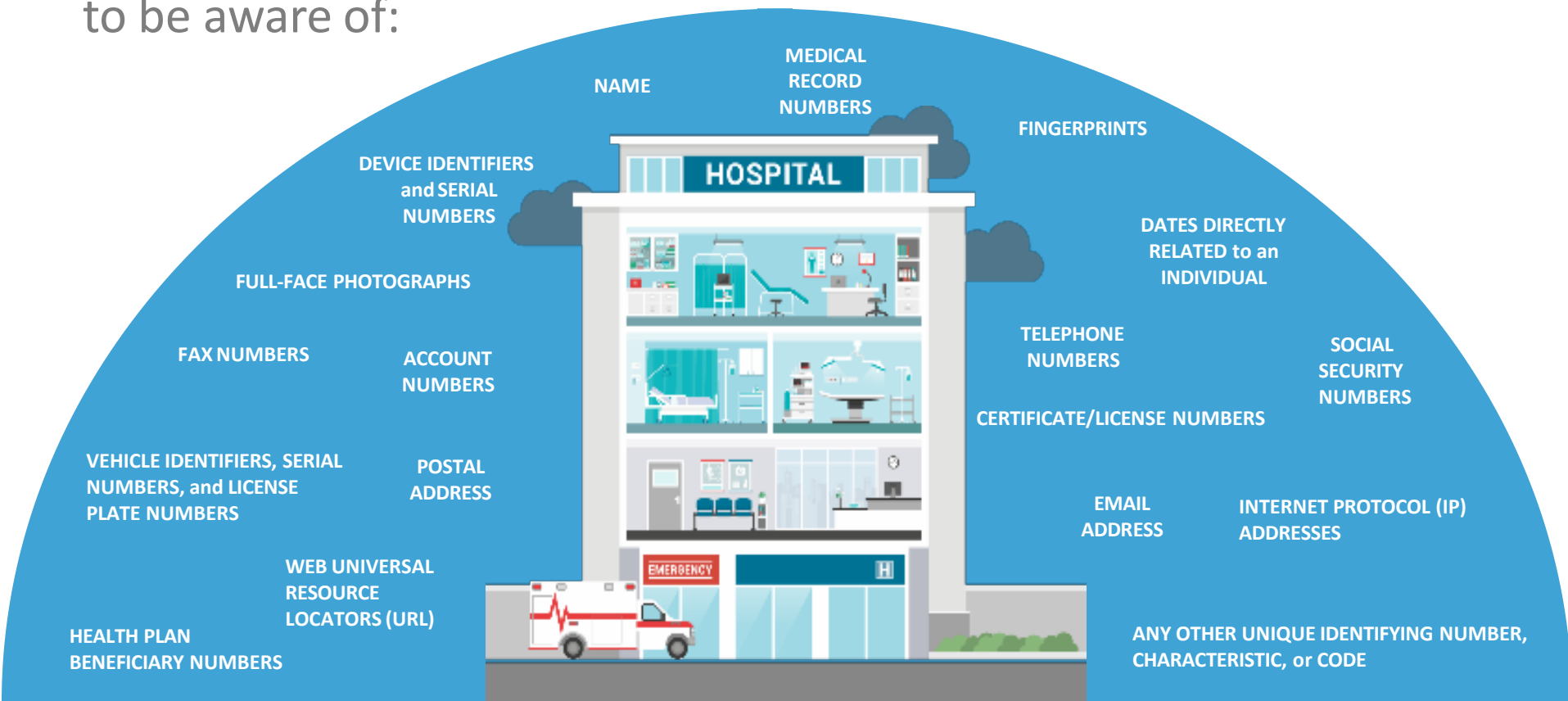
It also includes other personal information, like **payment information**

We must always be aware of PHI and work together to protect sensitive information



Where Can I Find PHI?

There are 18 PHI identifiers that Banner Health professionals need to be aware of:



It is important to understand that PHI is everywhere

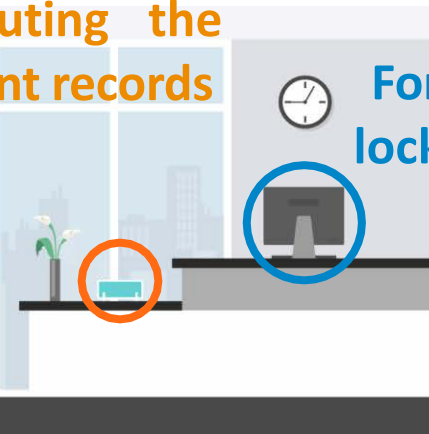
What Are Some Common Mistakes When Handling PHI?

Most PHI violations are not malicious, but are the result of unintentional human error, including:

Discussing patient information in public spaces



Printing, uploading, and distributing the wrong patient records



Forgetting to lock computer screens

Even if it is an accident, these are all HIPAA violations!

If you accidentally access an incorrect record or mishandle information, please **report it to your supervisor immediately**



What Are Other PHI Data Storage and Sharing Errors?

The most common mistakes made when handling PHI include:



SOCIAL MEDIA

- Be aware of what appears in photo backgrounds, is PHI displayed?
- Do not take pictures of patients, even if their face is not visible
- Never share any sensitive information in a public forum



UNSECURE EMAIL

- Encrypt all emails containing sensitive information that you send to a non-Banner Health email address
- Do not click any links or download attachments in suspicious emails or from unsecure websites



CLOUD STORAGE

- Do not store Banner Health information on an unapproved cloud platform
- Do not share cloud log in information or grant access to an unauthorized user

If you accidentally violate the guidelines above or mishandle PHI, report it to your supervisor immediately

What Are the Risks if PHI is Exposed?

If PHI is exposed and the HIPAA Privacy Rule or Security Rule is violated, consequences can be severe, including:

- Obligation to report to Office of Civil Rights (OCR)
- Fines and sanctions
- Corrective action and compliance
- Data breaches
- Loss of trust
- Loss of brand reputation for Banner Health



Follow [Information Security and Privacy policies](#) to make sure you are always in compliance

What Can I Do to Protect PHI?

Your job is to protect Banner Health and its patients, health plan members, and staff, which includes taking care of their PHI

Be aware when you handle PHI, including printed records, digital material, and conversations

Only use Banner Health approved systems and cloud platforms

Be careful of everything that you post on social media, and double check for PHI

Encrypt emails that you send to non-Banner Health email addresses



Reach out to your supervisor with any concerns

Follow the [Information Security and Privacy policies](#) to make sure you are always in compliance

Where Can I Find More Information?

For more details and the latest information, refer to the Banner Health policies located on the [intranet](#)



- [MobilePASS Self Service](#)
- [MyHR](#)
- [Online Event Reporting](#)
- [Paging Tool](#)
- [Password Reset Tool](#)
- [Patient Education](#)
- [Phone Lists](#)
- [Policies & Procedures](#)
- [Regulatory Program](#)
- [Report a HIPAA Privacy Incident](#)
- [Report a Work Injury/Exposure](#)
- [Report an Issue to the IT Service Desk](#)
- [Request Center](#)
- [TMA iService Desk](#)
- [Workforce Central](#)
- [Workforce Messaging](#)

In addition to reaching out to your supervisor, you can contact InformationSecurity-PrivacyTrainingandAwareness@bannerhealth.com with any questions

Dissemination

- Email
- Staff Meetings
- Facility Meetings
- Department Meetings
- eNews
- Yammer
- Blog



Q&A

