Banner Health Information Security and Privacy Training Team

Morgan Raimo
Paul Lockwood

Banner Health

PHI Storage InfoGraphics

Banner Health

Banner Health

PHI Data Storage and Sharing

Cybersecurity and Privacy Training and Awareness

Table of Contents

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**

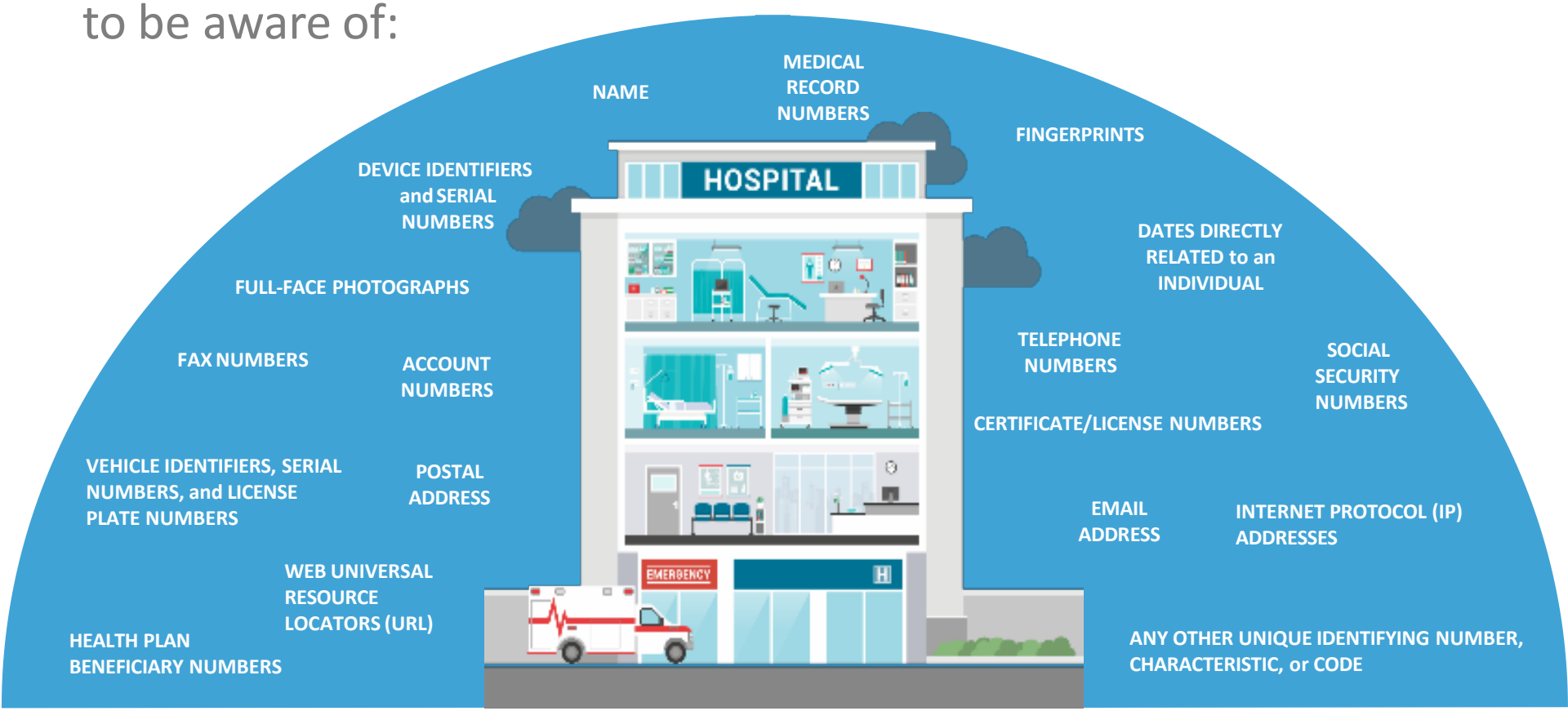
It also includes other personal information, like **payment information**

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

Banner Health

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

Banner Health

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

Banner Health

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

Banner Health

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

Banner Health

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

Banner Health

Where Can I Find More Information?

For more details and the latest information, refer to the Banner Health policies located on the intranet

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

Banner Health

Dissemination

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

Q&A