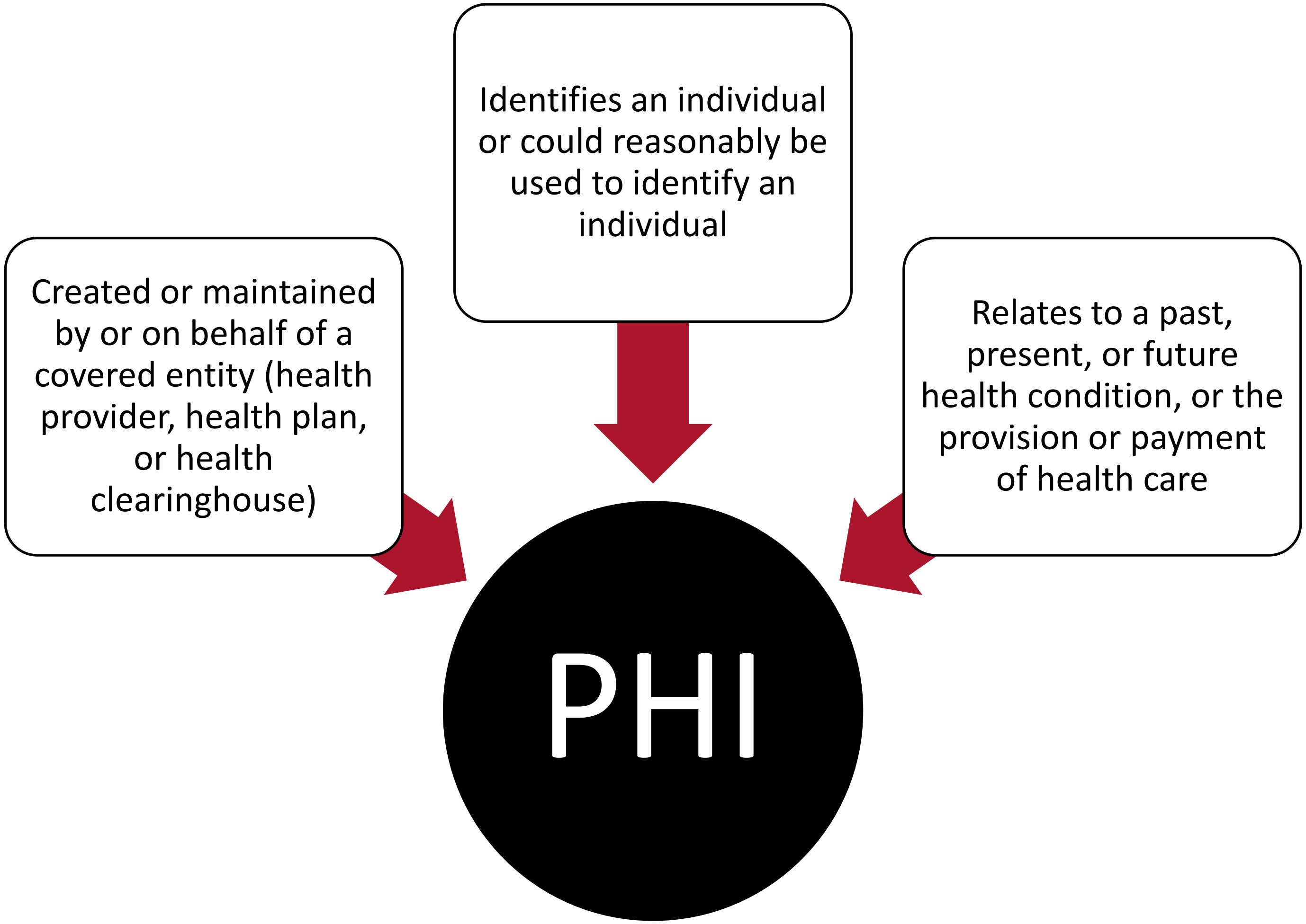
PROTECTING PHI IN RESEARCH

RQCN Compliance Cafe

HIPAA Compliance in Research

- De-identification.
- Device and data security.
- Data maintained outside of EMR.
- Compliant communications (for recruitment or other purposes).
- Reporting incidents.

What is PHI?



Identifies an individual or could reasonably be used to identify an individual

Created or maintained by or on behalf of a covered entity (health provider, health plan, or health clearinghouse)

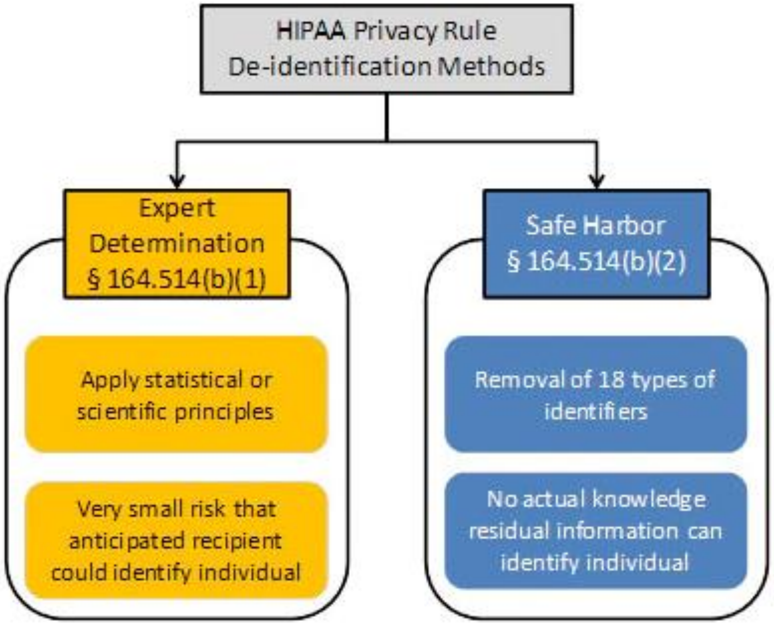
Relates to a past, present, or future health condition, or the provision or payment of health care

De-Identified PHI

The HIPAA Privacy Rule provides 2 acceptable methods to de-identify PHI:

1. Expert Determination Method
2. Safe Harbor Method

De-identified PHI is not subject to HIPAA Privacy and Security rules.



HIPAA Privacy Rule
De-identification Methods

Expert Determination
§ 164.514(b)(1)

Apply statistical or scientific principles

Very small risk that anticipated recipient could identify individual

Safe Harbor
§ 164.514(b)(2)

Removal of 18 types of identifiers

No actual knowledge residual information can identify individual

Expert Determination Method

Requires that a qualified expert determine the risk is very small that the information could be used, alone or in combination with other reasonably available information, to identify an individual who is a subject of the information.

1. The qualified expert must use generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.
2. The method used to justify the determination must be documented.
3. The expert must provide a written certification indicating the time frame during which the expert's determination remains valid.

Safe Harbor Method

The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed:

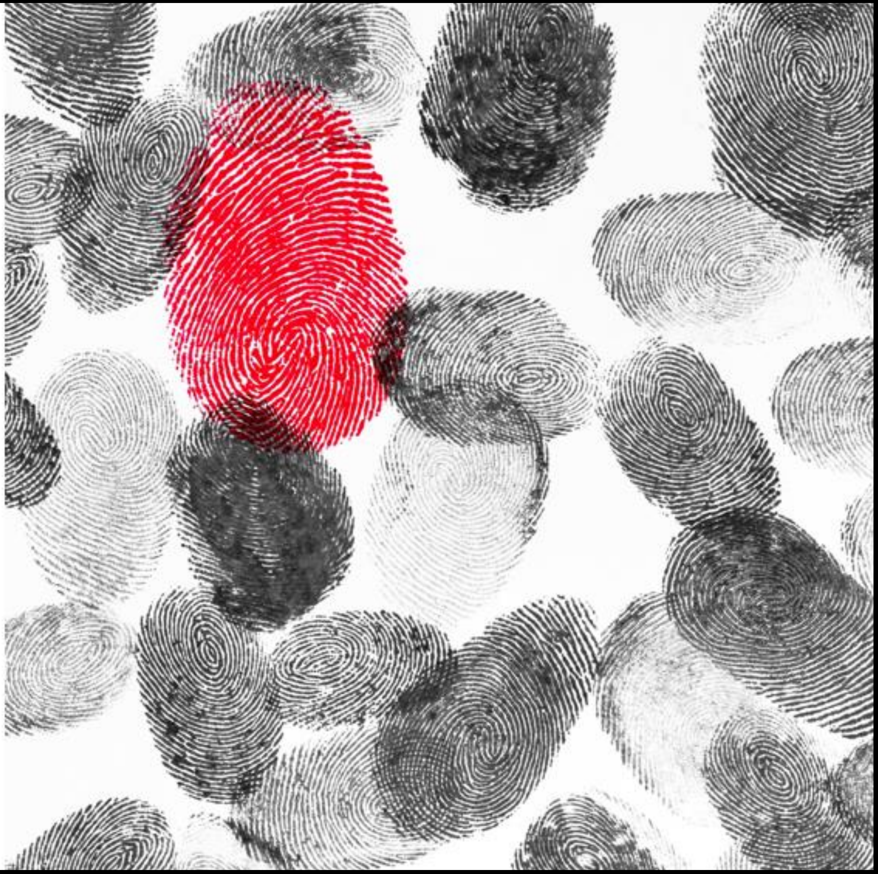
- Names
- Geographic subdivisions smaller than a State
- All elements of dates (except year)
- Telephone numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs)
- SSNs
- IP addresses
- Medical record numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any other unique identifying number, characteristic, or code
- Certificate/license numbers

Identifies an Individual

- Names
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual

Other Identifying Characteristics

- Demographics such as age, gender, race, ethnicity, LGBTQIA identification, number of children, marital status.
- Photos that include intimate areas of a patient’s anatomy, profile photos, images showing unique injuries, health conditions, or unique physical attributes.
- Details about a patient’s social/personal history (e.g., incarceration, housing status, substance use, occupation, socioeconomic status).



DATA ELEMENTS ARE LIKE PUZZLE PIECES

The more pieces you combine, the more identifiable the picture becomes.

May parts or derivatives of any of the listed identifiers be disclosed with the Safe Harbor Method?

If data contains patient initials, last four digits of Social Security number, or other derivatives, this **does not** meet the Safe Harbor method for de-identification.

What are examples of dates that are not permitted according to the Safe Harbor Method?

Not Permitted	Permitted
✗ August 25, 2024	✓ 2024
✗ 90 years old	✓ 90 or above
✗ DOS- 1993	✓ Before 1995

Limited Data Set

- A data set that excludes all of the safe harbor direct identifiers of the patient, or relatives, employers or household members of the patient, **except:**
  - Dates, such as admission, discharge, service, date of birth, date of death.
  - City, state, five digit or more zip code.
  - Ages in years, months, days or hours.
- A limited data set may only be used or disclosed for the purposes of research, public health, or health care operations.
- U of U Health may use or disclose a LDS if it enters into **Data Use Agreement** with the recipient.

⚠ *NOT DE-IDENTIFIED AND IS SUBJECT TO HIPAA*

Information Security

PHI must be encrypted at rest and in transit, meaning:

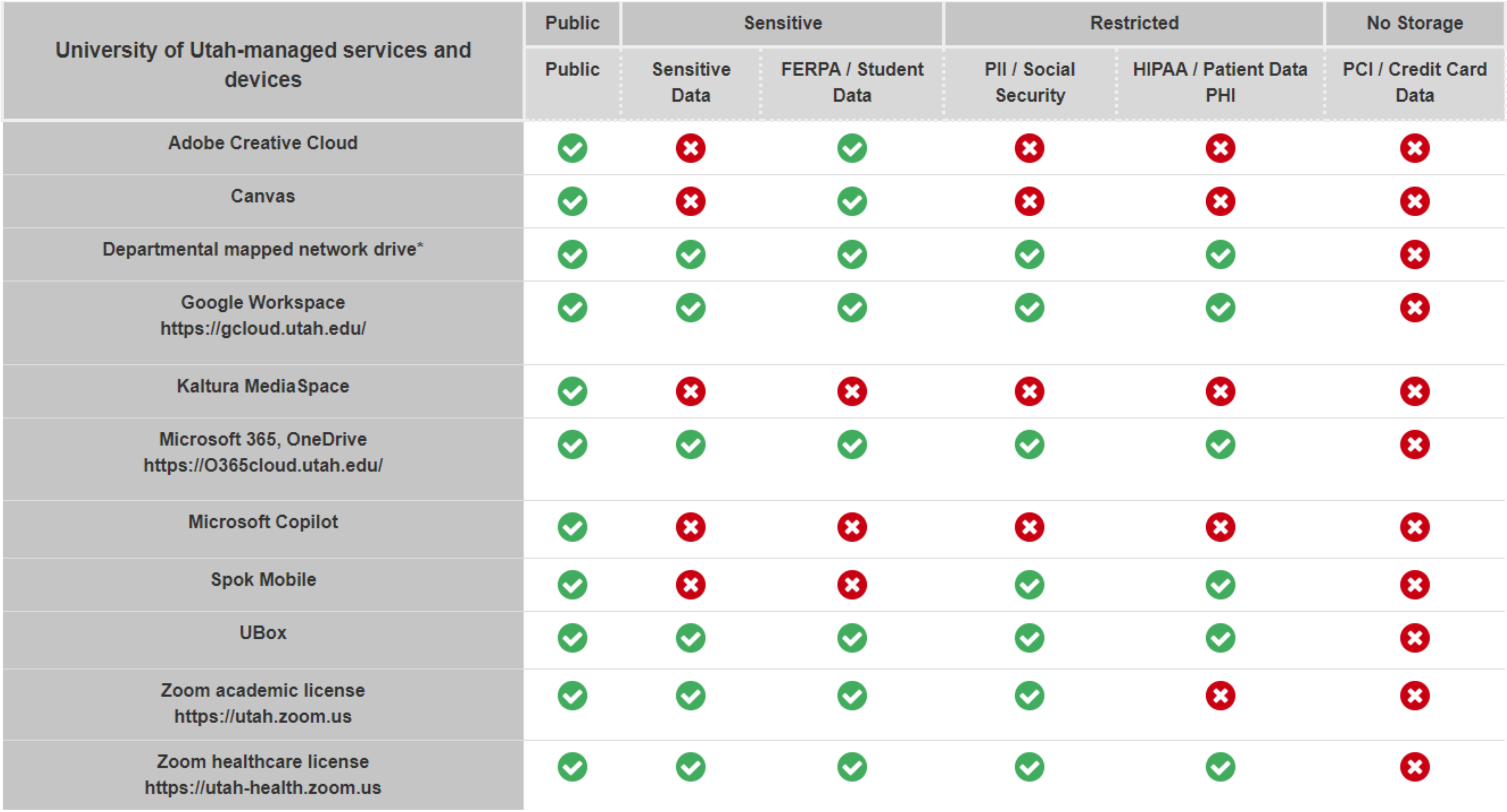
- All devices storing, processing, creating, or transmitting PHI shall be encrypted
- PHI can only be stored and shared on University-approved platforms
- Emails containing PHI must be encrypted

Secure Devices

- Personally owned devices (or BYOD) are subject to the same state and federal regulations as a device owned and maintained by U of U Health.
- Use a university-managed device or work with IT or ISO to have security tools installed on your personal device.

Please see the Tip Sheet on Restricted Data and Personal Devices.

University-approved data sharing platforms



University of Utah-managed services and devices	Public	Sensitive		Restricted		No Storage
	Public	Sensitive Data	FERPA / Student Data	PII / Social Security	HIPAA / Patient Data PHI	PCI / Credit Card Data
Adobe Creative Cloud	✓	✗	✓	✗	✗	✗
Canvas	✓	✗	✓	✗	✗	✗
Departmental mapped network drive*	✓	✓	✓	✓	✓	✗
Google Workspace https://gcloud.utah.edu/	✓	✓	✓	✓	✓	✗
Kaltura MediaSpace	✓	✗	✗	✗	✗	✗
Microsoft 365, OneDrive https://O365cloud.utah.edu/	✓	✓	✓	✓	✓	✗
Microsoft Copilot	✓	✗	✗	✗	✗	✗
Spok Mobile	✓	✗	✗	✓	✓	✗
UBox	✓	✓	✓	✓	✓	✗
Zoom academic license https://utah.zoom.us	✓	✓	✓	✓	✗	✗
Zoom healthcare license https://utah-health.zoom.us	✓	✓	✓	✓	✓	✗

What if the platform I use is not on this list?

If you're sharing PHI with third party vendors, there are a few methods of approval:

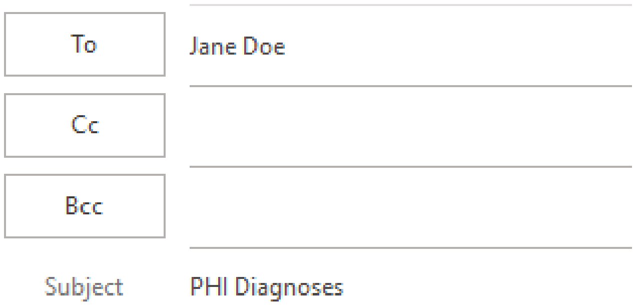
- ✓ You're processing a Limited Data Set and have a Data Use Agreement
- ✓ You're processing PHI and have a Business Associate Agreement
- ✓ The third-party vendor is listed on the Informed Consent document
- ✓ You're processing De-identified Data

If you're unsure, contact the Privacy Office ☺

Email Encryption

- Emails containing PHI must be encrypted by putting "PHI" in the subject line as shown.
- Encrypting emails encrypts the body of the message and not the subject line. Do not include any PHI in the subject line such as patient's name, DOB, or MRN in the subject line of emails.

✓



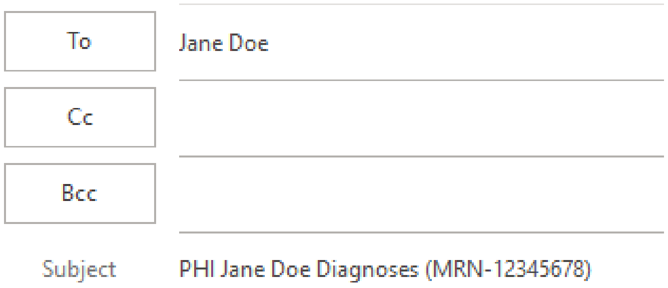
To: Jane Doe

Cc:

Bcc:

Subject: PHI Diagnoses

✗



To: Jane Doe

Cc:

Bcc:

Subject: PHI Jane Doe Diagnoses (MRN-12345678)

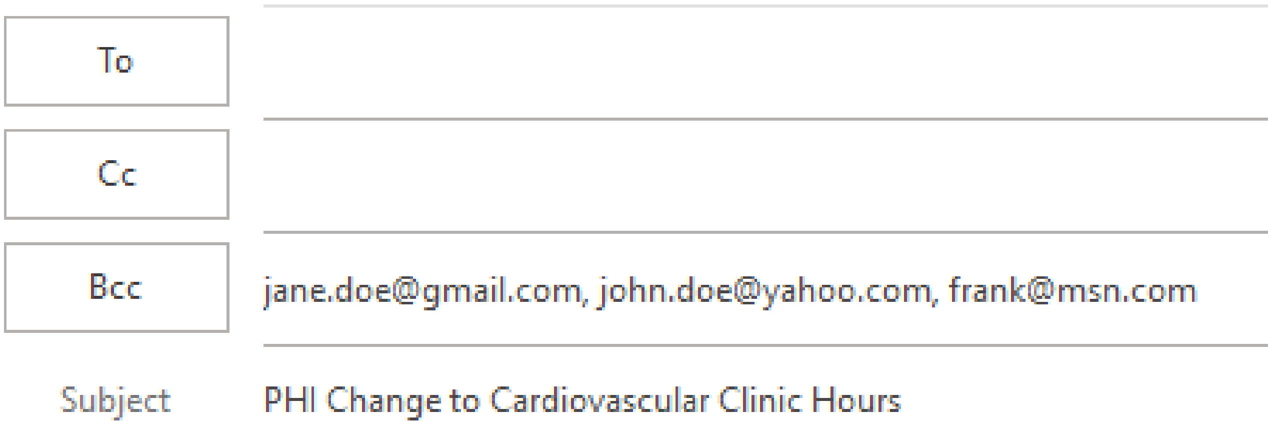
Emailing Large Amounts of PHI

When sharing large amounts of PHI, avoid sending this data via email.

Instead, we recommend using UBox or Microsoft OneDrive as a more secure method of sharing data.

Blind Carbon Copy

When sending an email to multiple patients, BCC (Blind Carbon Copy) recipients email addresses. Doing this keeps patients' email address private from other recipients.



Bcc jane.doe@gmail.com, john.doe@yahoo.com, frank@msn.com

Subject PHI Change to Cardiovascular Clinic Hours

Personal Email Use

- In accordance with University Policy 4-010, all employees must only use UMail accounts to conduct University business.
  - This includes emails going to colleagues or other employees within the university.
- Auto-forwarding messages from your UMail to your personal email address is prohibited.

Summary

- Understand what your data is classified as under the HIPAA Privacy Rule (De-identified vs. PHI)
- Check that your devices are secure and meet University Policy
- Only use University-approved platforms to store and share PHI
- Email PHI encrypted and avoid sharing large amounts of PHI via email

Contact the Privacy Office

Send an email to
privacy@utah.edu

Call the Privacy Office at
801-587-9241

Report a privacy incident
at privacy.utah.edu

Resources

- HHS Guidance on Research
- Rule R4-004C: Data Classification and Encryption
- Information Privacy Policies
  - Policy: HIPAA: De-Identification and Re-Identification of Protected Health Information (PHI) and Limited Data Sets
  - Policy: HIPAA: General Policy Regarding the Privacy and Security of Protected Health Information (PHI)