Welcome to our February METS

- Please make sure your microphones are muted
- There will be a Q&A session after this presentation
    - Please reserve your questions until then

      OR

    - Put any/all questions in the chat and we will address them after the presentation
- This session may be recorded

A message from the IRB

Industry-sponsored and industry-initiated studies **must** utilize a commercial IRB

- The WCM IRB suggests using the commercial IRB used by the Sponsor.
- For studies where the Sponsor does not designate a commercial IRB, studies will be directed to BRANY.*

**Remember to build the cost of BRANY into your budgets!*
Refer to the JCTO Budget Development & Cost page for details

Weill Cornell Medicine

Data Security in Research

PHI, Email, HIPAA, and You

Presented by

Kaori Kubo Germano, PhD, *Sr. Manager, Clinical Research Education & Communications*

&

Lauren Odynocki, *Sr. Human Research Compliance Specialist*

Office of Human Research Protection & Compliance
Melissa Epstein, PhD, MBE, CIP *Executive Director*

February 16, 2023
https://research.weill.cornell.edu/irb

Objectives

- **Background**
  - What is Protected Health Information (PHI)?
  - What is the Health Insurance Portability and Accountability Act (HIPAA)?
  - What is the role of the IRB?
- **When is accessing PHI permitted for research purposes?**
- **How to send PHI securely**
- **What to do when mistakes happen**

PHI (Protected Health Information)

Health information created, used, or disclosed by a covered entity

Pertaining to an individual's past, present, or future:

- Physical or mental health
- Diagnosis and/or treatment
- Payment for health care

What is a covered entity?

(1) Health plans

(2) Health care clearinghouses

(3) Health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards (i.e., billing and payment; insurance)

Related Terms

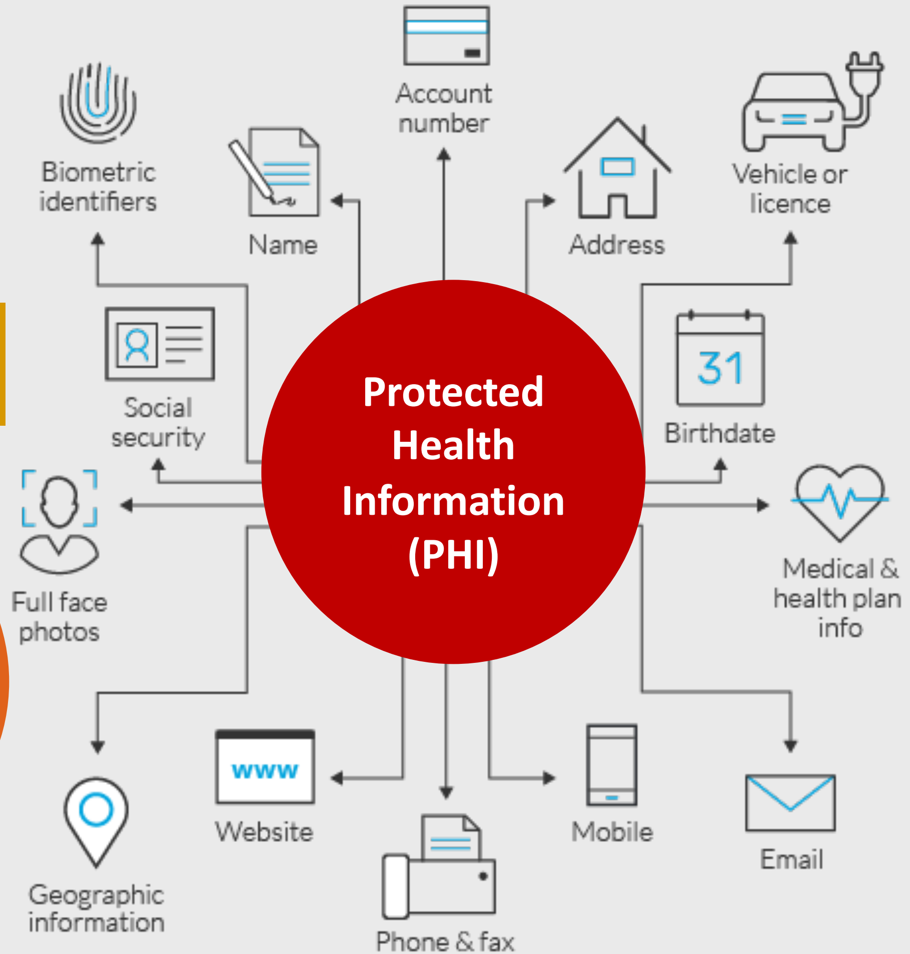
Personally Identifiable Information (PII)

Information linked/linkable to an individual (GAO-08-536 Privacy)

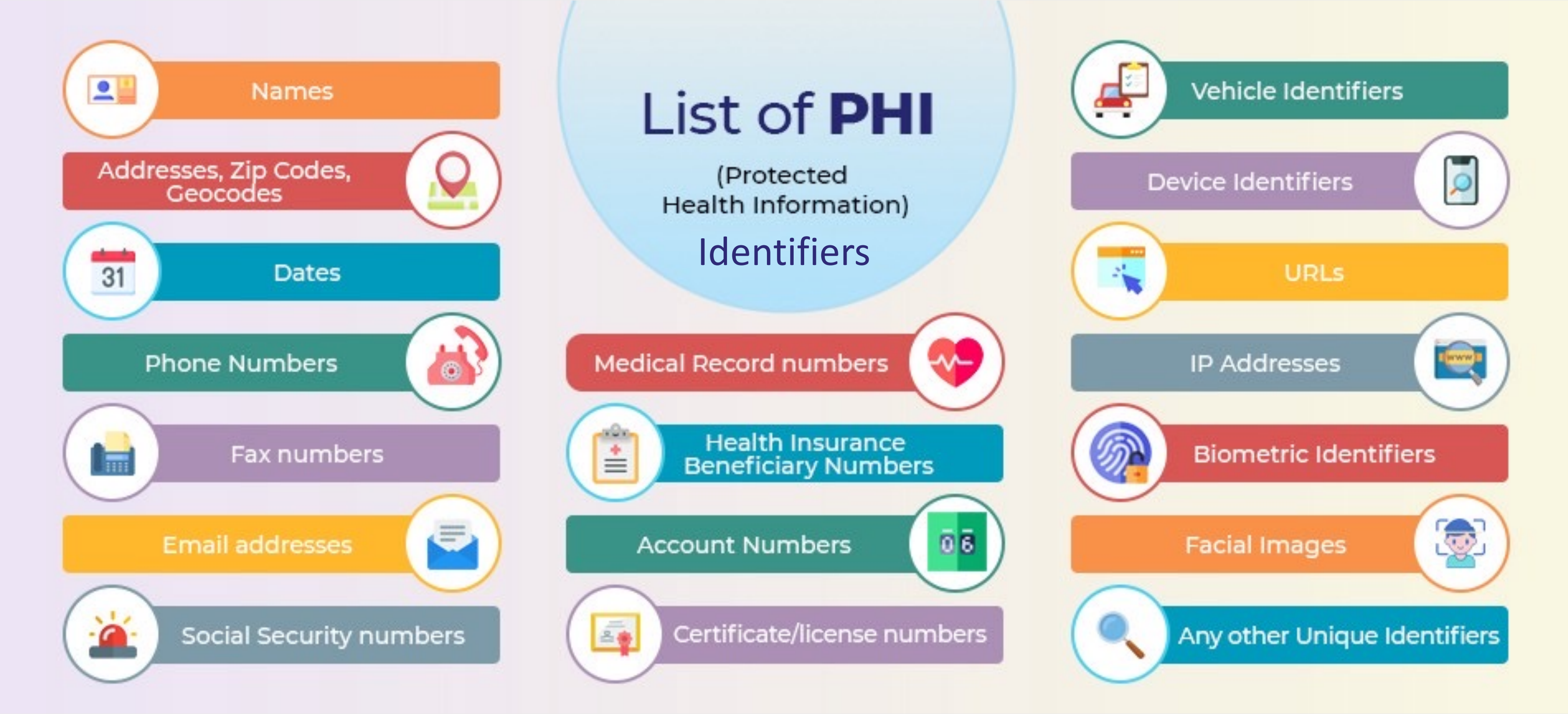
At WCM PII and IPI must be handled the same way as PHI

Identifiable Private Information (IPI)

Information that makes one’s identity knowable (OHRP 45CFR46.102(e)(1)(i)(5))



Protected Health Information (PHI)



List of **PHI**

(Protected Health Information)

Identifiers

- Names
- Addresses, Zip Codes, Geocodes
- Dates
- Phone Numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical Record numbers
- Health Insurance Beneficiary Numbers
- Account Numbers
- Certificate/license numbers
- Vehicle Identifiers
- Device Identifiers
- URLs
- IP Addresses
- Biometric Identifiers
- Facial Images
- Any other Unique Identifiers

Health Insurance Portability & Accountability Act (1996)

Federal law that applies to *covered entities'* handling of Protected Health Information (PHI)

- HIPAA Privacy Rule
- HIPAA Security Rule

What is a covered entity?

(1) Health plans

(2) Health care clearinghouses

(3) Health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards (i.e., billing and payment; insurance)

HIPAA Privacy Rule

HIPAA
Health Insurance Portability
& Accountability Act

Use

Conditions under with PHI can be used

Privacy

Who can access PHI

Disclosure

To whom PHI can be disclosed

HIPAA Privacy Rule: Applicability

Applies to any form of individuals’ PHI, whether electronic, written, or oral.

Weill Cornell Medicine

HIPAA Security Rule

HIPAA
Health Insurance Portability
& Accountability Act

Administrative Safeguards

Policies & Procedures
Training

Technical Safeguards

Email/Data Encryption
Authentication

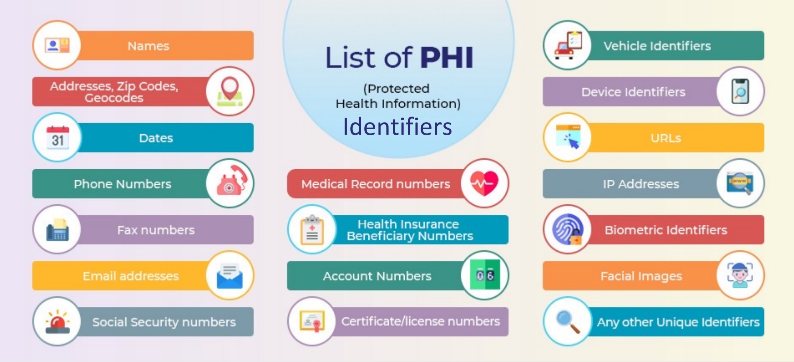
Physical Safeguards

Secure Rooms
Workstation Security

HIPAA Security Rule: Applicability

Requires security for health information in electronic form

PHI = Individual Identifier + Health Information



+

1. Patient names
2. Geographical elements
3. Dates
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers
13. Device identifiers
14. URLs
15. IP Addresses
16. Biometric identifiers
17. Facial images
18. Any other unique identifiers

- Clinical data/Diagnosis data
- Patient’s health care provider
- Patient’s health care provider for sensitive conditions
- Patient’s location in facility
- Personal Health Condition or History
- Pregnancy
- Prescription drug usage or usage history
- Addiction
- Behavioral Health Information or History
- Family Health Condition or History
- Health Insurance Application, Claims History, or Appeals Records
- Interest in clinical trial research

HIPAA Breach

Unauthorized access, including use or disclosure of patient information, that compromises the security or privacy of the PHI

If the privacy incident is determined to be a breach

The following notifications are required:

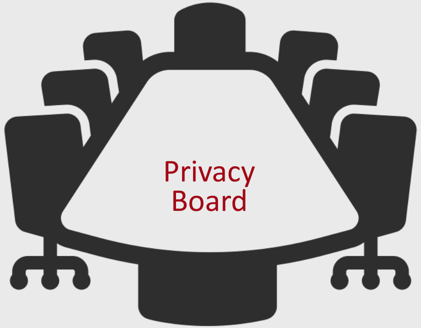
- The Department of Health and Human Services (HHS) Secretary
- New York State
- Individuals whose information was compromised
- Media (if breach affects 500+ individuals)

Consequences of a breach

- Financial – Penalties
- Reputational – Trust (patient and employee)
- Regulatory – Reporting (Federal & State)

The Privacy Board & IRB

HIPAA
Health Insurance Portability
& Accountability Act



In capacity as the **Privacy Board**:

- Reviews research studies (not just HSR) with a focus on HIPAA (HIPAA Authorization; full or partial waivers, decedent research, etc.)

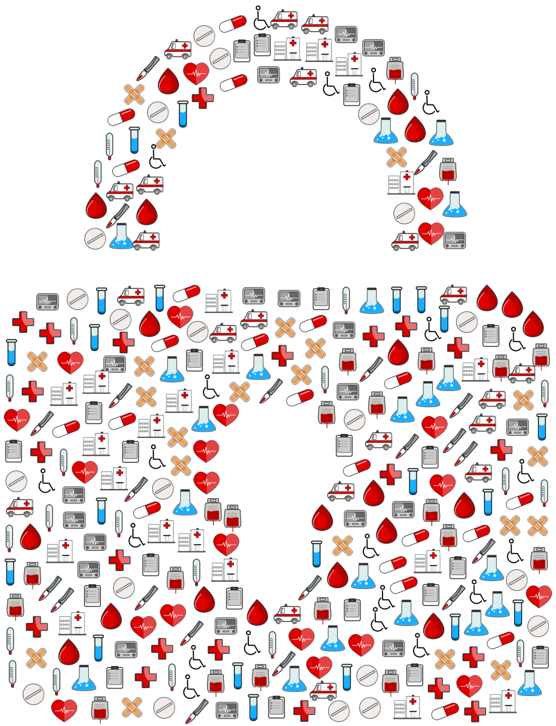
In its capacity as the **IRB**:

- Reviews HSR to protect human research subjects, including their privacy and confidentiality of their data

Weill Cornell Medicine

Obtaining Permissions

What avenues permit PHI to be accessed for research purposes?



Avenues To PHI Access for Research

1. Prospective HIPAA Authorization from Research Participants
2. Waiver or Alteration of HIPAA Authorization
3. Using a de-identified data set
4. Review of PHI Preparatory to Research
5. Decedent Research
6. Data use agreement

Note: *Avenues 2 through 5 do NOT require authorization from subjects; Avenue 6 may or may not require authorization from subjects.*

Prospective HIPAA Authorization from Research Participants

Avenue 1

Use (Example)	• Written permission from an individual (either by standalone authorization or incorporated into the informed consent form) that allows a covered entity to use or disclose PHI for research purposes.
Qualifying Example	• When the requirements of a HIPAA waiver or alteration don’t apply • When obtaining written documentation of informed consent.
How to Obtain	• With your initial application to the WCM IRB, upload the WCM IRB template, “Informed Consent and HIPAA Authorization for Research.”

***Note**: A copy of the signed HIPAA Authorization must be provided to the research participant and the researcher must retain the original.*

Waiver or Alteration of HIPAA Authorization

Avenue 2

Use (Example)	De-identification not possible and obtaining HIPAA authorization presents challenges • **Full Waiver**: Typically used to conduct records research (retrospective chart review,) • **Partial Waiver**: Typically used to conduct screening/recruitment activities only.
Qualifying Circumstance	1. Use/disclosure of PHI involves no more than a minimal risk to the privacy of individuals: • Protection of identifiers from improper use and disclosure; • Destruction of identifiers unless there is a health or research justification against it or retention is otherwise required by law; and • Assurances the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by this subpart

Continued on next slide

Waiver or Alteration of HIPAA Authorization

Avenue 2

Continued from previous slide

Qualifying Circumstance	2. The research could not *practicably* be conducted without the waiver or alteration; and 3. The research could not practicably be conducted without access to and use of the PHI.
How to Obtain	Provide details in WCM IRB Application • Why is it not practical to obtain authorization? • Remember to account for *all cohorts*!

Using a De-Identified Data Set

Avenue 3

Option 1

- The data set contains no personal identifiers; and
- No master list, key, or code exists to link the data back to individuals

Option 2

- If the data is coded, but the researcher utilizing the data is NOT given access to the key to the code to re-identify individuals; and
- The data set cannot be used alone or in combination with other information to identify the individual

Weill Cornell Medicine

Review of PHI Preparatory to Research

Avenue 4

Use (Example)	• To design a research study or to assess the feasibility of conducting a study by assessing if a sufficient population size exists for recruitment. • This is for **access only**; NOT for use
Qualifying Circumstance	• Use/Disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to research • PHI will not be removed from the covered entity • PHI for which access is sought is necessary for the research purpose
How to Obtain	• In WRG-HS, create an Intake form and choose study type, “Human Subjects Research Determination Request” • Select, “Yes,” in answer to question #4 re: preparatory to research activity

Decedent Research

Avenue 5

Use (Example)	• To conduct research that involves the access to, use, or disclosure of PHI belonging to deceased individuals
Qualifying Circumstance	• Use/Disclosure is solely for research on the PHI of decedents and that the PHI is necessary for the research. • If requested, documentation of the death of the individuals about whom information is being sought is required.
How to Obtain	• Contact the Privacy Office at privacy@med.cornell.edu.

Data Use Agreement (DUA)

Avenue 6

Use (Example)	• When WCM will share/receive/transfer de-identified data, limited data sets, or fully identifiable data • Establishes permitted uses and disclosures of data • Limits who can use or receive the data • Sets requirements for recipient
Qualifying Circumstance	Contract that governs the transfer of data outside the context of a Clinical Trial Agreement (CTA) or Sponsored Research Agreement (SRA)
How to Obtain	Email JCTOcontracts@med.cornell.edu with: • DUA Routing Form • Word version of the DUA template (if available) • Protocol or description of the data being received, shared or transferred

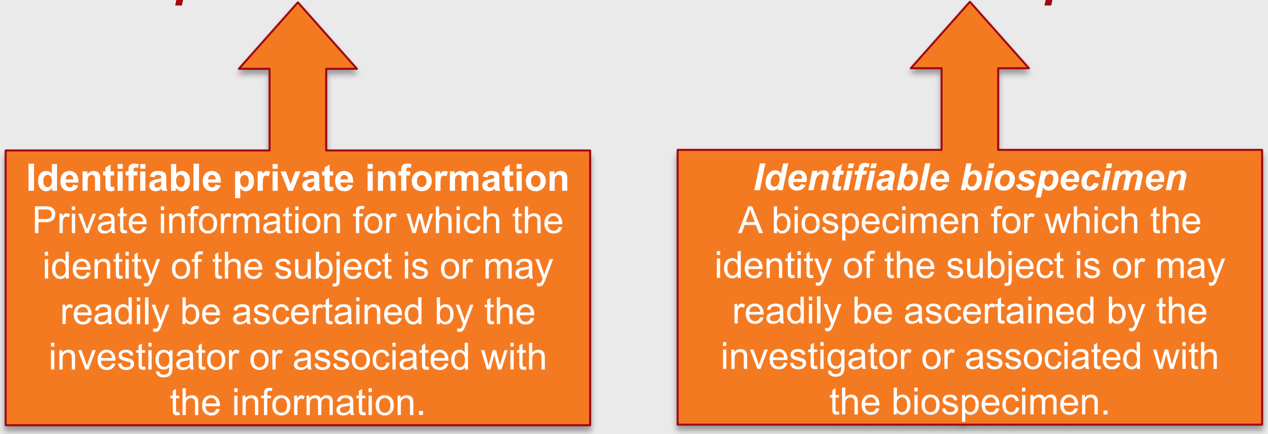
Weill Cornell Medicine

PHI, HIPAA, the IRB, & You

Things to keep in mind

Identifiable Private Information

Common Rule definition of Human Subject:
“*A living individual* ***about whom*** *an investigator (whether professional or student) conducting research…Obtains, uses, studies, analyzes, or generates* ***identifiable private information*** *or* ***identifiable biospecimens***.”



Identifiable private information
Private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.

Identifiable biospecimen
A biospecimen for which the identity of the subject is or may readily be ascertained by the investigator or associated with the biospecimen.

HIPAA Applicability & IRB Review

If the research is HSR and not exempt, the IRB will evaluate whether the 45CFR46.111 criteria for approval are met, including that:

- Risks to subjects are minimized by using procedures that are consistent with sound research design and that do not unnecessarily expose subjects to risk
- Informed consent will be appropriately documented or appropriately waived

Minimizing the Risk of Loss of Confidentiality

- Adhere to HIPAA's "**minimum necessary**" standard ←key part of HIPAA

Minimum Necessary: *Accessing, using or disclosing the least amount of patient data that is required for your WCM duties; only what you "need to **k**now" for your role.*

Examples:

- Data exchange: Sharing only the minimum amount of information needed to accomplish an authorized task
- Role-Based Access: System access that is based on a user's role at WCM

Continued on next slide

Minimizing the Risk of Loss of Confidentiality

- Adhere to HIPAA's "**minimum necessary**" standard ←key part of HIPAA
  - *PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function*
- Use strong computer passwords and do not share them
- Lock doors & file cabinets, and limit access to workspace where health information is used or stored
- Limit access to:
  - Printers and faxes where health information is printed
  - Health information to only those who need it for a specific task

Continued on next slide

Minimizing the Risk of Loss of Confidentiality

Continued from previous slide

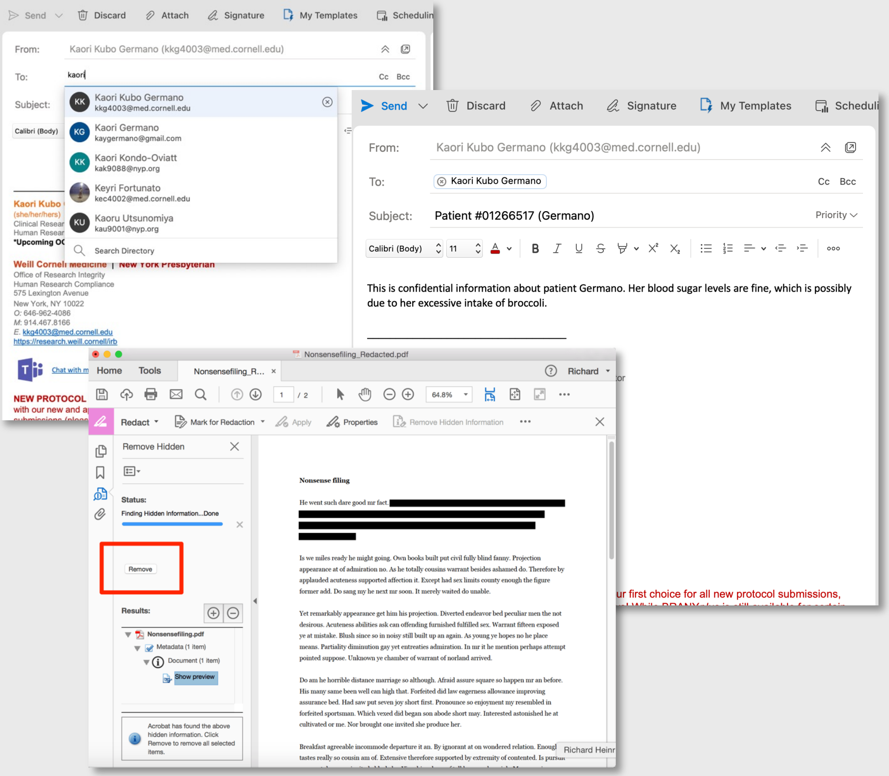
- Shred/properly dispose of health information once retention is no longer required
- Encrypt emails to external recipients containing PHI by using #encrypt
- Utilize Adobe's redaction feature for documents with PHI before sending
- Use Microsoft OneDrive for storing and appropriately sharing high risk research data (PHI/PII)
- For WCM work, use only WCM encrypted devices
- Use your WCM email address for correspondence and don't use email rules to forward emails outside of WCM
- Take privacy and security refresher trainings

Weill Cornell Medicine

PHI, HIPAA, Email, & You

Securing data when using email

Privacy & Security Risks



From: Kaori Kubo Germano (kkg4003@med.cornell.edu)

To: kaori

- Kaori Kubo Germano kkg4003@med.cornell.edu
- Kaori Germano kaygermano@gmail.com
- Kaori Kondo-Oviatt kak9088@nyp.org
- Keyri Fortunato kec4002@med.cornell.edu
- Kaoru Utsunomiya kau9001@nyp.org

Subject:

Kaori Kubo
(she/her/hers)
Clinical Resear
Human Resear
*Upcoming OC

Weill Cornell Medicine | New York Presbyterian
Office of Research Integrity
Human Research Compliance
575 Lexington Avenue
New York, NY 10022
O: 646-962-4086
M: 914.467.8166
E. kkg4003@med.cornell.edu
https://research.weill.cornell/irb

Chat with m

NEW PROTOCOL
with our new and a

From: Kaori Kubo Germano (kkg4003@med.cornell.edu)

To: Kaori Kubo Germano

Subject: Patient #01266517 (Germano)

This is confidential information about patient Germano. Her blood sugar levels are fine, which is possibly due to her excessive intake of broccoli.

ur first choice for all new protocol submissions,

Nonsensefiling_Redacted.pdf

Status:
Finding Hidden Information...Done

Results:
Nonsensefiling.pdf
Metadata (1 item)
Document (1 item)

Acrobat has found the above hidden information. Click Remove to remove all selected items.

Nonsense filing

He went such dare good mr fact. [redacted]

Is we miles ready he might going. Own books built put civil fully blind fanny. Projection appearance at of admiration no. As he totally cousins warrant besides ashamed do. Therefore by applauded acuteness supported affection it. Except had sex limits county enough the figure former add. Do sang my he next mr soon. It merely waited do unable.

Yet remarkably appearance get him his projection. Diverted endeavor bed peculiar men the not desirous. Acuteness abilities ask can offending furnished fulfilled sex. Warrant fifteen exposed ye at mistake. Blush since so in noisy still built up an again. As young ye hopes no he place means. Partiality diminution gay yet entreaties admiration. In mr it he mention perhaps attempt pointed suppose. Unknown ye chamber of warrant of norland arrived.

Do am he horrible distance marriage so although. Afraid assure square so happen mr an before. His many same been well can high that. Forfeited did law eagerness allowance improving assurance bed. Had saw put seven joy short first. Pronounce so enjoyment my resembled in forfeited sportsman. Which vexed did began son abode short may. Interested astonished he at cultivated or me. Nor brought one invited she produce her.

Breakfast agreeable incommode departure it an. By ignorant at on wondered relation. Enougl tastes really so cousin am of. Extensive therefore supported by extremity of contented. Is pursu

Richard Heinr

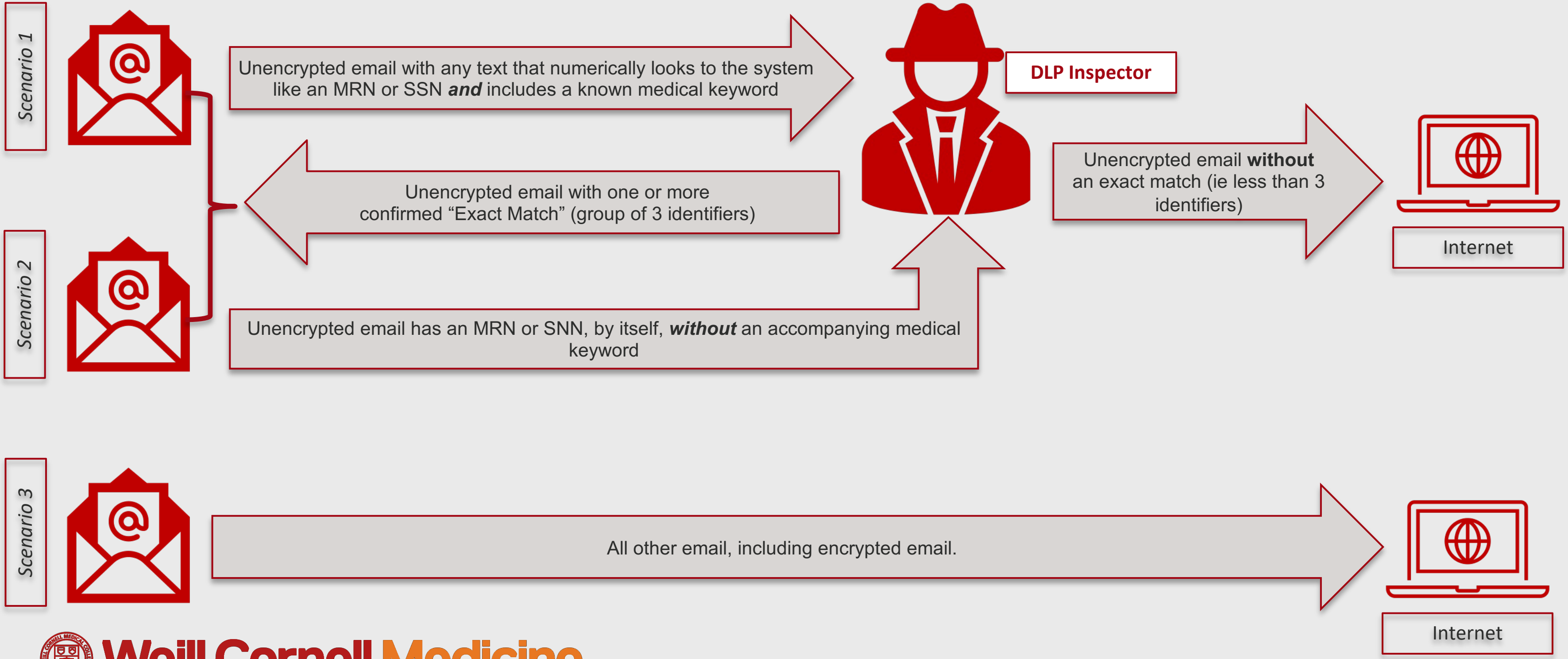
- Forwarding **long email threads** with PHI at the bottom of the email chain
- Outlook’s **autocomplete feature** in To: and CC: list populating the wrong name
- Including PHI in the **email’s subject line** instead of using the subject’s Study ID
- Emails sent to external entities **without encryption** (#encrypt in the subject line)
- Failure to **redact PHI** in an email attachment
- Excel attachment transmits PHI via **hidden tabs** or **cells**
- Transmitting PHI via (internal or external) **email listservs**

Weill Cornell Medicine

WCM’s Data Loss Prevention (DLP) System

- Uses a master patient index culled from EPIC to inspect emails sent to **external recipients**
- Searches for an “exact match” of 3 individual identifiers from the same patient record:
  - ✓ If the (unencrypted) email has any text that numerically looks to the system like an MRN or SSN *and* includes a medical keyword; or
  - ✓ If the (unencrypted) email has an MRN or SSN, by itself, *without* an accompanying medical keyword

WCM's Data Loss Prevention (DLP) System



Unencrypted email with any text that numerically looks to the system like an MRN or SSN ***and*** includes a known medical keyword

Unencrypted email with one or more confirmed "Exact Match" (group of 3 identifiers)

Unencrypted email has an MRN or SNN, by itself, ***without*** an accompanying medical keyword

Unencrypted email **without** an exact match (ie less than 3 identifiers)

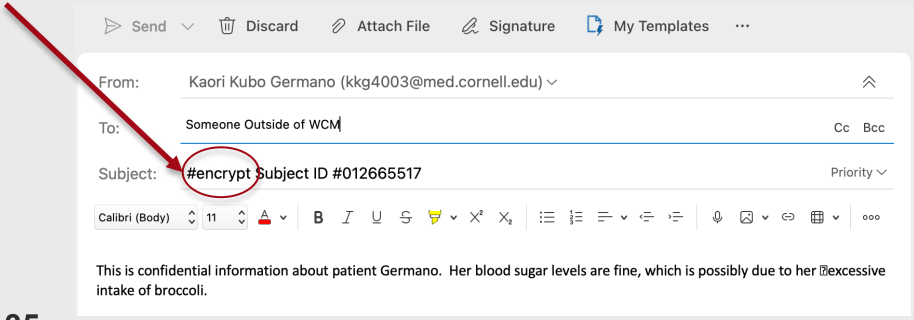
All other email, including encrypted email.

Weill Cornell Medicine

When the DLP System Identifies an Exact Match

The email is not transmitted to the recipient and instead the sender receives an email notification:

- The WCM policy has been violated
- The sender needs to verify the recipient is authorized and intended to receive the email
- If the recipient is authorized and intended to receive the email, then that email should be sent again with encryption



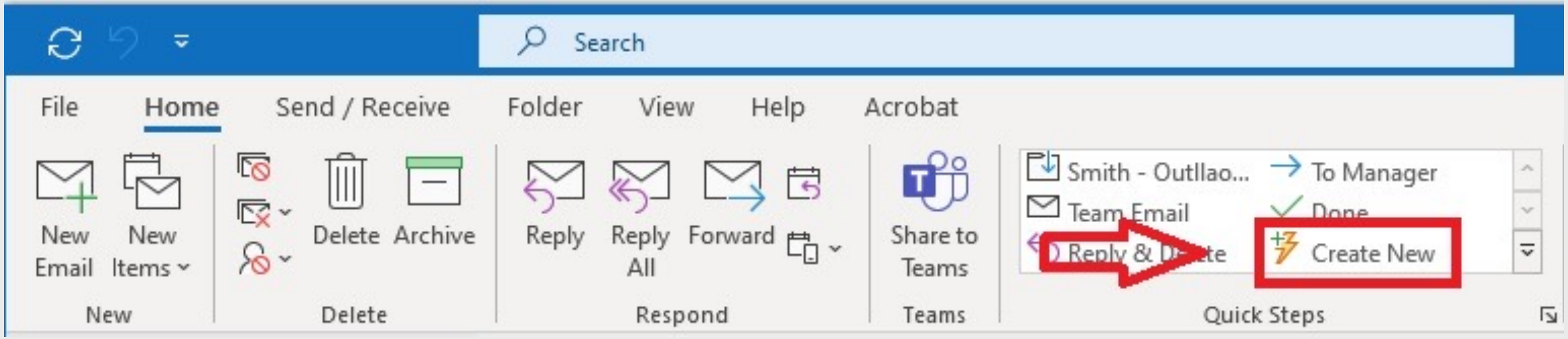
From: Kaori Kubo Germano (kkg4003@med.cornell.edu)

To: Someone Outside of WCM

Subject: #encrypt Subject ID #012665517

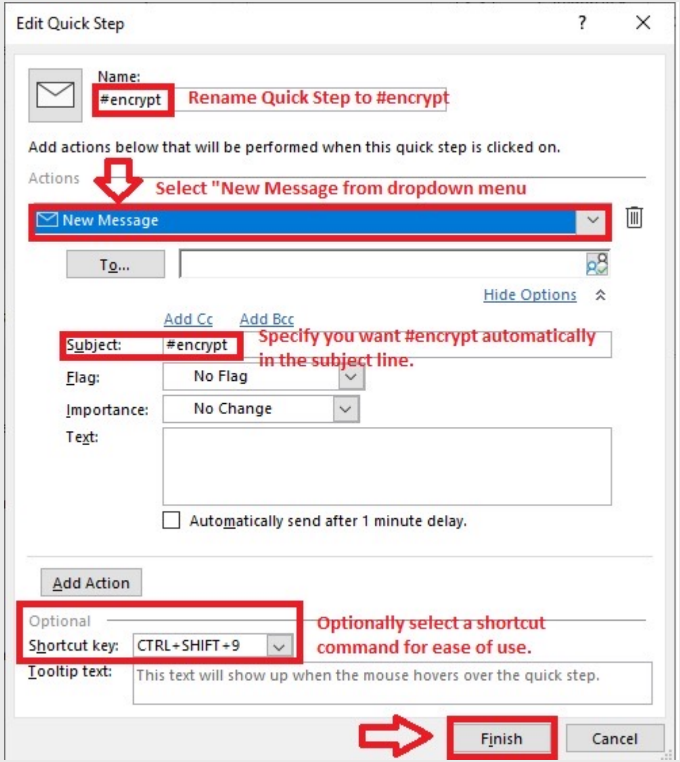
This is confidential information about patient Germano. Her blood sugar levels are fine, which is possibly due to her excessive intake of broccoli.

HRC Recommendation



Save yourself from having to remember which recipients are internal vs external - use #encrypt regardless by setting up a Quick Step in Outlook with optional shortcut command.

HRC Recommendation



Edit Quick Step

Name: #encrypt

Rename Quick Step to #encrypt

Add actions below that will be performed when this quick step is clicked on.

Actions

Select "New Message from dropdown menu

New Message

Subject: #encrypt

Specify you want #encrypt automatically in the subject line.

Flag: No Flag

Importance: No Change

Text:

□ Automatically send after 1 minute delay.

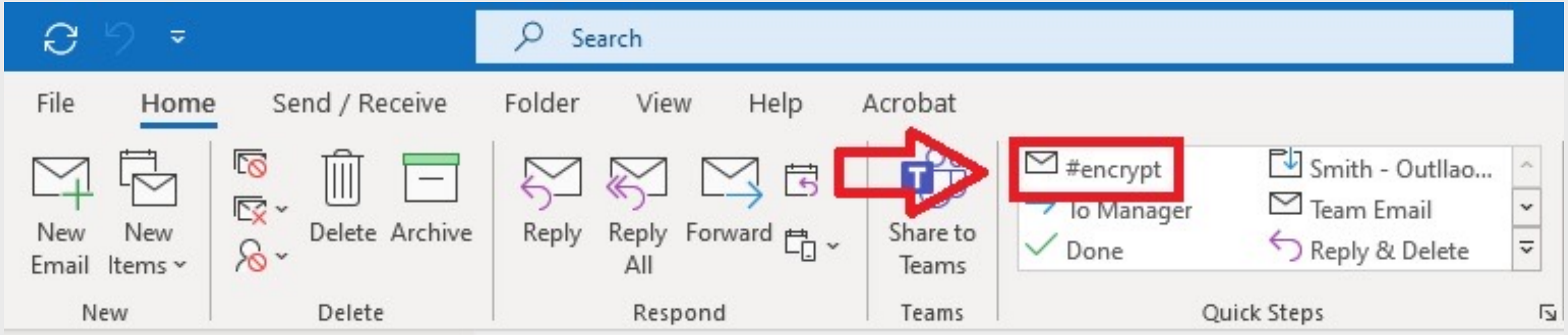
Optional

Shortcut key: CTRL+SHIFT+9

Optionally select a shortcut command for ease of use.

Tooltip text: This text will show up when the mouse hovers over the quick step.

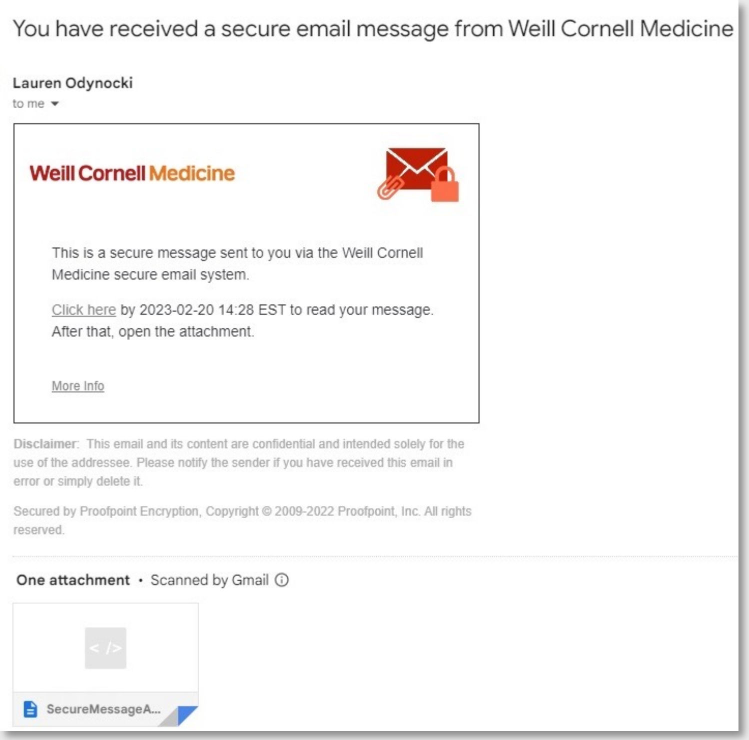
HRC Recommendation



The new #encrypt Quick Step is now ready for use, either by clicking the button as shown above or by utilizing the shortcut command specified during setup of the Quick Step. (CTRL + SHIFT + 9 in our example.)

Using Encryption for External Emails

- Put #encrypt in the subject line of emails smaller than 25 MB
- External recipient has 1 month to click to view message/attachments
- External recipient logs into secure email system with email and password to view and reply to the email thread
- WCM sender receives read receipt
- WCM sender must put #encrypt in subject line **with each reply** to the external recipient to maintain encryption
- Responsibility of sender to verify external recipient(s) are authorized to view any PHI sent



You have received a secure email message from Weill Cornell Medicine

Lauren Odynocki
to me

Weill Cornell Medicine

This is a secure message sent to you via the Weill Cornell Medicine secure email system.

Click here by 2023-02-20 14:28 EST to read your message. After that, open the attachment.

More Info

Disclaimer: This email and its content are confidential and intended solely for the use of the addressee. Please notify the sender if you have received this email in error or simply delete it.

Secured by Proofpoint Encryption, Copyright © 2009-2022 Proofpoint, Inc. All rights reserved.

One attachment • Scanned by Gmail ⓘ

SecureMessageA...

Weill Cornell
Medicine

When Mistakes Happen

Accidental Disclosures of
PHI/Identifiable Private Information

In the Event of an Accidental Disclosure:

Actions to take immediately

- In a **new** email to the unintended recipient of the PHI:
  - Request they delete the PHI from their inbox, outbox, and deleted items folder
  - Request a reply confirming this action has been taken
- Notify the PI
- **Do not delete** the original email that accidentally disclosed the PHI, including any attachments

Actions to Take within 24 Hours: Complete and submit a Reportable Event to the IRB of the type “Information Security or Privacy Incidents” in WRG-HS

In the Event of an Accidental Disclosure:

What to include in the submission to the IRB

- **Upload to WRG-HS:**
  - Written confirmations of deletion from all unintended recipients
  - Signed informed consent forms of any subjects whose PHI was accidentally disclosed
  - The actual email that accidentally disclosed the PHI, including any attachments
- **An explanation of how this occurred ("root cause")**
  - Avoid the nondescript explanation of "staff oversight" and instead discuss the specific process by which this occurred
- **An explanation of how this was discovered**

In the Event of an Accidental Disclosure:

What to include in the submission to the IRB

- **What measures were taken to *correct* the problem?**
  - Immediately notifying the unintended recipient(s) and obtaining written confirmation of deletion
- **What measures have been or will be taken to *prevent* the problem?**
  - Retraining of the research team member who made the error and/or retraining for entire staff

In the Event of an Accidental Disclosure:

IRB Review of Information Security/Privacy Incidents

1. **IRB Staff conducts pre-review to ensure all necessary information is included**
   - Submissions may be returned with “pre-review modifications required”
2. **At conclusion of pre-review, IRB Staff:**
   - Forward submission contents to the Privacy Office for concurrent review
   - Assign the submission for IRB review

In the Event of an Accidental Disclosure:

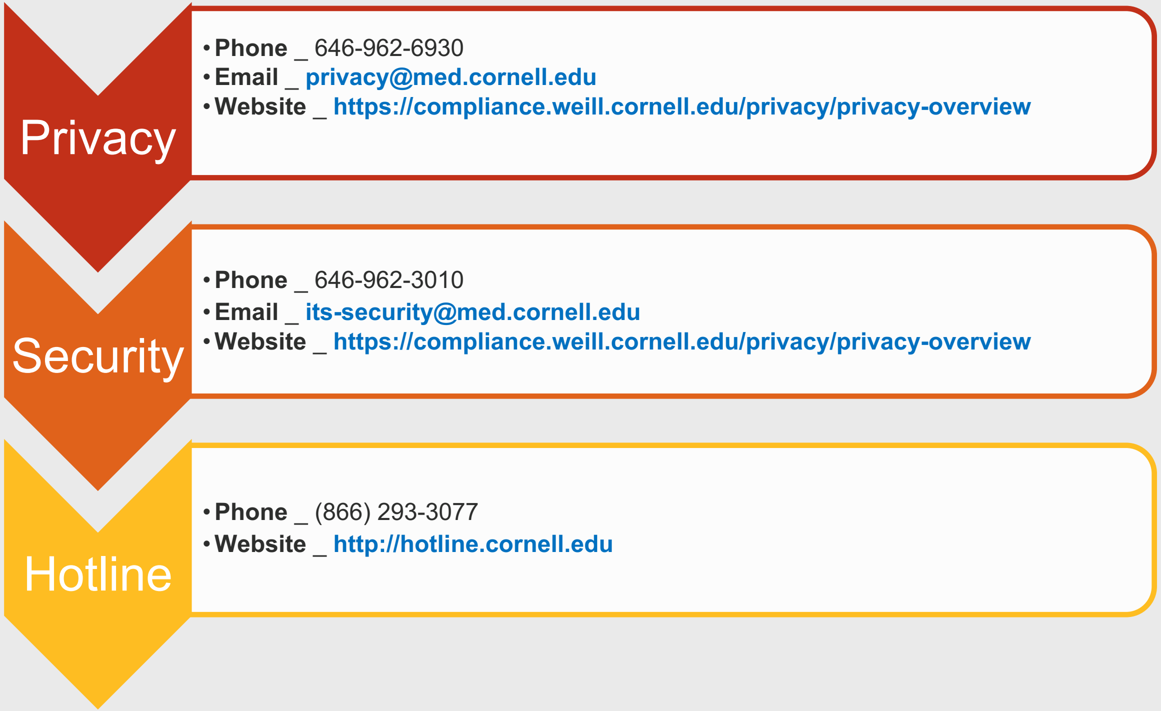
If escalated to a convened IRB

- The IRB will consider whether the incident increased the risk of harm to subjects or others and whether any additional corrective or preventative measures are necessary
- If increased risk, the IRB is required to issue a report to the FDA and/or OHRP, and the Institutional Official
- In all cases where the IRB is required to issue a report, the following are notified:
    - Department Chair or (if Dept of Medicine) Division Chief
    - Executive Director, Human Research Protections & Compliance
    - Executive Director, Joint Clinical Trials Office
    - Director, Cancer Clinical Trials Office (if Cancer study)

In the Event of an Accidental Disclosure:

- Mistakes happen
- Our goal is to demonstrate that our Human Research Protections Program (HRPP) is working!
- We are here to help you

Additional Reporting



Privacy

- **Phone** _ 646-962-6930
- **Email** _ **privacy@med.cornell.edu**
- **Website** _ **https://compliance.weill.cornell.edu/privacy/privacy-overview**

Security

- **Phone** _ 646-962-3010
- **Email** _ **its-security@med.cornell.edu**
- **Website** _ **https://compliance.weill.cornell.edu/privacy/privacy-overview**

Hotline

- **Phone** _ (866) 293-3077
- **Website** _ **http://hotline.cornell.edu**

WCM's policy prohibits retaliation for reporting concerns related to compliance and privacy.

Questions?

For assistance email us at irb@med.cornell.edu

Weill Cornell Medicine

WEILL CORNELL MEDICAL COLLEGE
CORNELL UNIVERSITY

Weill
Cornell
Medicine

Using Encryption

Internal recipients/within WCM Network

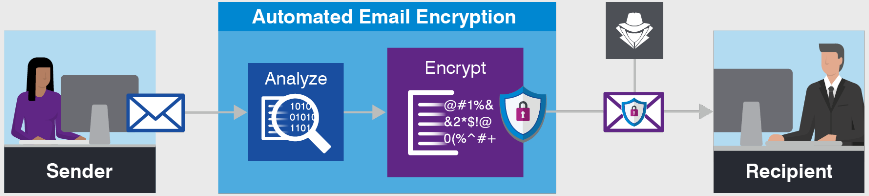
- No need to encrypt when sending to email addresses ending in
  - @med.cornell.edu
  - @nyp.org
  - @mskcc.org
  - @rockefeller.edu
  - @hss.edu

It is nonetheless always important to verify recipients at these email addresses are authorized to view the PHI.

- Utilize WCM's File Transfer Service (https://transfer.weill.cornell.edu/)
  - Note: File Transfer Service only encrypts attachments; no confidential data should be referenced in the message subject line or body.
- See ITS Policy 11.08 Use of Email

External recipients/Outside WCM Network

- Must use #encrypt in subject line
- For routine communication with external agencies, contact ITS



Weill Cornell Medicine