



# Overview of HIPAA Privacy & Information Security Requirements Related to Research

January 28, 2022

RESEARCH



## Research Investigator Workshop

# Objectives

- Provide guidance on BCM Policy on Uses and Disclosures of PHI for Research purposes
- Describe what is de-identified PHI
- Provide guidance on BCM Information Security Requirements

# What health information is protected by the Privacy Rule?

*The Privacy Rule applies to protected health information (PHI) created or maintained by a Covered Entity (and a CE business associates)*

- ***What is PHI?***

- Individually identifiable health information (IIHI)  
**AND**
- Transmitted or maintained in any form or medium (i.e., verbal, paper or electronic)

- **What is IIHI**

- Information that relates to past, present or future physical or mental health or condition; healthcare; or payment for healthcare  
**AND**
- Identifies an individual or can reasonably can be used to identify  
**AND**
- Created or received by a covered entity (healthcare provider, health plan, or clearinghouse)

# General Premise

- A PHI is private and confidential and cannot be disclosed by BCM UNLESS:
  - There is a valid Written Authorization;
  - It is for Payment, Treatment or Healthcare Operations (TPO); or
  - When Required by law or Otherwise Allowed by law.

# Treatment, Payment and Health Care Operations (TPO)

**Treatment**: various activities related to patient care.

**Payment**: various activities related to paying for or getting paid for health care services.

**Health Care Operations**: generally refers to day-to-day activities of a covered entity, such as planning, management, education and training, quality improvement, accreditation, peer review.

**NOTE**: *Research is **not** considered TPO.*

# Protected Health Information (PHI)

Protected Health Information (PHI) includes the following identifiers:

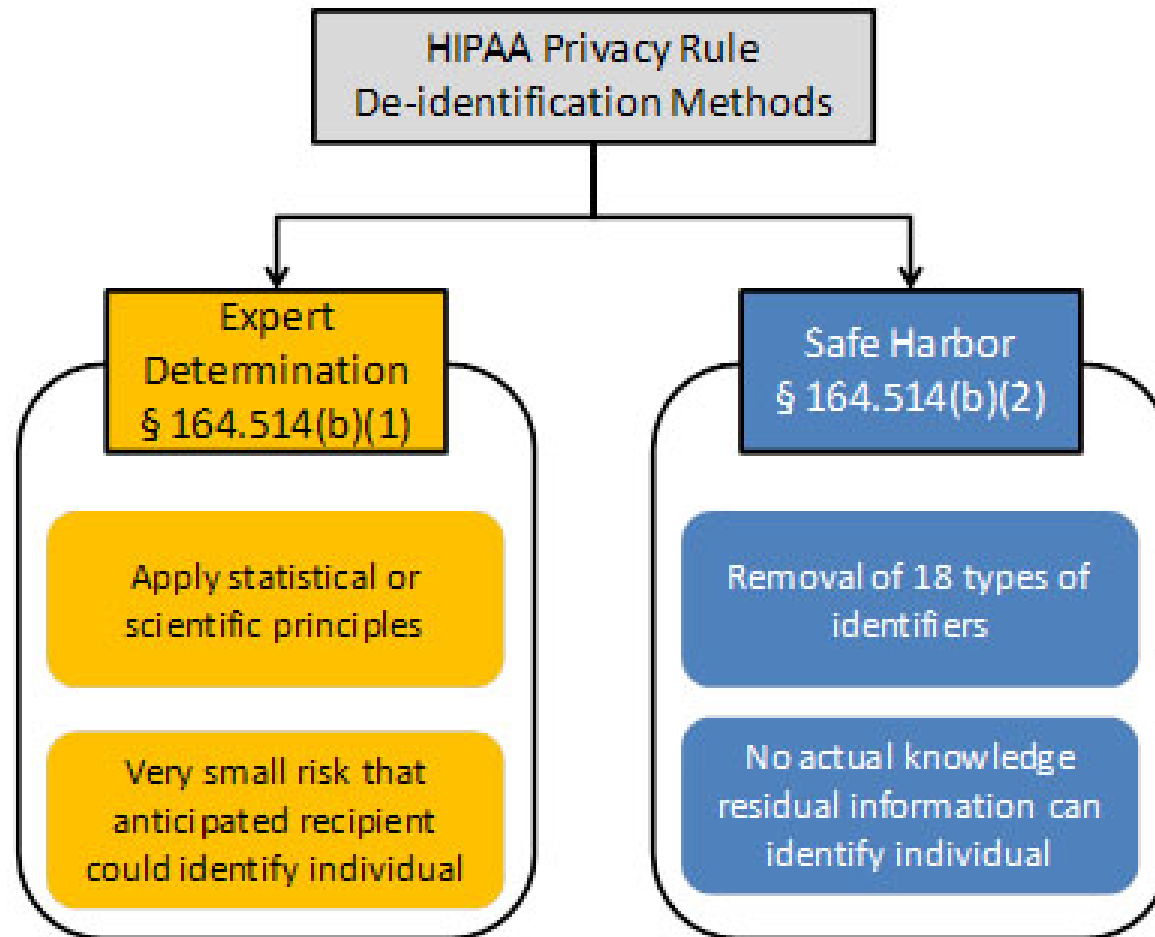
Name	Vehicle identifiers and serial numbers, including license plate numbers	Device identifiers and serial numbers
All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes,	Social security numbers	Web Universal Resource Locators (URLs)
All elements of dates (except year) for dates directly related to an individual	Medical record numbers	Internet Protocol (IP) address numbers
Telephone numbers	Health plan beneficiary numbers	Biometric identifiers, including finger and voice prints
Fax numbers	Account numbers	Full face photographic images and any comparable images
Electronic mail addresses	Certificate/license numbers	<b>Any other unique identifying number, characteristic, or code and the covered entity has no reasonable basis to believe it can be used to identify an individual.</b>

Information does not need to include diagnosis or treatment information to be considered PHI.

# De-Identified PHI

- Information that cannot be used to identify an individual is not protected.
- How to de-identify information:
  - Hire an expert to determine that information to be used or disclosed contains no identifying information.
  - Remove all specified identifying information.

# De-identification Methodologies





# Protected Health Information (PHI)

- What constitutes “any other unique identifying number, characteristic, or code” with respect to the Safe Harbor method of the Privacy Rule?
  - This category corresponds to any unique features that are not explicitly enumerated in the Rule, but could be used to identify a particular individual. Thus, a covered entity must ensure that a data set stripped of the explicitly enumerated identifiers also does not contain any of these unique features. The following are examples of such features:

# Protected Health Information (PHI)

- Identifying Number - Clinical trial record numbers
- Identifying Code - An increasing quantity of electronic medical record and electronic prescribing systems assign and embed barcodes into patient records and their medications. These barcodes are often designed to be unique for each patient, or event in a patient's record, and thus can be easily applied for tracking purposes.
- Identifying Characteristic - A characteristic may be anything that distinguishes an individual and allows for identification. For example, a unique identifying characteristic could be the occupation of a patient, if it was listed in a record as "current President of State University."

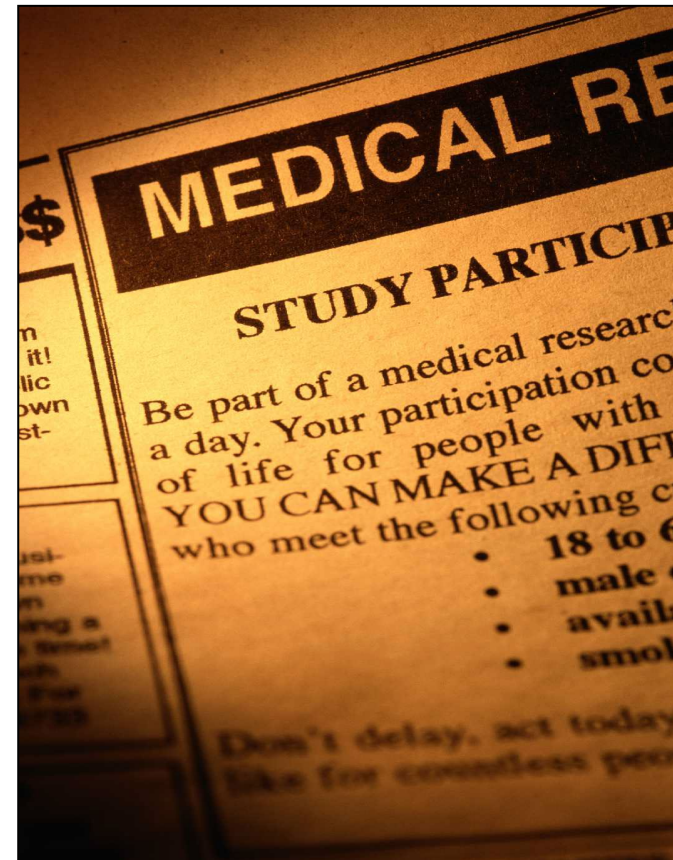
# Research: General Rule

## ◆ General Rule

PHI (for living or deceased individuals) may be used or disclosed for research purposes only with written “authorization” (permission) from the patient or his/her Legal Representative

# Research: Authorization Required

- ◆ Patient permission or “*authorization*” is usually needed to use or share PHI for research.
- ◆ Conduct of research generally is governed under federal regulations for the protection of human subjects (the “Common Rule”); and use or sharing of PHI for research is governed by HIPAA



# Exceptions to the Authorization Requirement

- **Authorization requirement is subject to some exceptions:**
  1. Waiver of authorization (approved by IRB)
  2. Use of PHI “preparatory to research”
  3. Use of decedents’ information for research purposes
  4. Disclosure of limited amounts of PHI under a “data use agreement”

# Preparatory to Research Activities

- BCM can Use and Disclose PHI for Reviews Preparatory to Research without authorization
  - Required Representations. Individuals seeking access to BCM PHI for reviews preparatory to research must provide the following written representations before accessing or given access to PHI:
    - The Use or Disclosure of PHI is solely to prepare a Research protocol or for similar purposes that are Preparatory to Research; and
    - The person agrees not to remove the PHI from BCM.
  - A statement describing the purposes for which the PHI is sought. For example, a feasibility analysis to determine the number of potential participants with a certain disease for submission in a grant, or identify potential research subjects in a study.
- **Requests for PHI for Activities Preparatory to Research must be made using the Request for PHI for Activities Preparatory to Research Form**

# Preparatory to Research

## Request for Access to PHI for Activities Preparatory to Research

I hereby request to review health records for the following research purpose (*researcher must indicate one of the purposes below*):

**Only Review Preparatory to Research** - I am solely assessing feasibility or preparing a research protocol and **I hereby represent that** (*Researcher must check all*):

- I will not record any individually identifiable PHI; and
- I will not remove any PHI from the records; and
- I will only review PHI that is necessary for this preparation for research; and
- I will not use PHI accessed in this review to prescreen individuals or make contact with individuals for recruitment or other research purposes. I understand that recruitment activities, including prescreening, may only be performed in accord with IRB review and approval.

Describe the proposed research: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Type of health information to which access is requested** (medical records, imaging studies, pathology information, lab information, etc.) and proposed review site:

- Electronic records: data base(s) to be reviewed: \_\_\_\_\_
- Paper records: site of review (location and department): \_\_\_\_\_
- Imaging studies: site of review (location and department): \_\_\_\_\_
- Other: \_\_\_\_\_

*Please describe your request below if OIT needs to generate the list for you. Otherwise, please attach the list of records you are requesting.*

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

# Preparatory to Research

*Please describe your request below if OIT needs to generate the list for you. Otherwise, please attach the list of records you are requesting.*

---

---

---

---

I acknowledge that:

- The requested information will only be used for activities preparatory to research.
- I agree that I will use only the information necessary for the research purpose described.
- I will protect the confidentiality and security of this information while it is in my possession, and will destroy identifiers if required by accompanying documentation.
- I understand and agree to comply with the obligations listed in this section as well as with all obligations described for the boxes I have checked above, and to inform all research team members of their responsibilities for compliance with these obligations.
- I will not remove the PHI from BCM premises.

\_\_\_\_\_  
*Signature of Principal Investigator*

\_\_\_\_\_  
*Date of Request*

\_\_\_\_\_  
*Print Name*

*Contact Information of Principal Investigator:*

---

---

---



# Preparatory to Research: Limited Use of PHI

- During the Preparatory to Research review, those granted access cannot remove any PHI from the location where PHI is stored. **Printing, copying, saving, or faxing PHI through remote access is considered removing the PHI from the particular BCM Department/Clinic.**
- BCM can allow an individual seeking access to PHI for reviews Preparatory to Research to identify and contact a potential study participant without authorization if:
  - The individual is a BCM Workforce Member and is contacting the potential participant as part of the BCM's Health Care Operations for purposes of seeking authorization.
  - The treating provider can discuss treatment alternatives which may include participating in a clinical trial as part of the patient's treatment or BCM's Health Care Operations.

# Preparatory to Research: Limited Use of PHI

- The BCM Workforce Member conducting the Review cannot delegate recruitment (contacting the patients/prospective research subjects) to anyone who is not a BCM Workforce Member.
- Uses or Disclosures of PHI for reviews that are Preparatory to Research are subject to:
  - The minimum necessary rules. See BCM Policy No. 31.4.07, Uses & Disclosures of PHI: Minimum Necessary Standard
  - Accounting of disclosures. See BCM Policy No. 31.4.xx, Right to an Accounting of Disclosures.

# Research on Decedents' PHI

- BCM can allow Access to and/or Disclose PHI of decedents solely for research purposes without a HIPAA Authorization or IRB Waiver of Authorization provided that the individual seeking access to decedents' PHI provide the following written representations:
  - Written statement from the Individual that the PHI will be solely used for Research and the PHI sought is necessary for conducting the Research;
  - Documentation of the patient(s) death by providing the patient's death certificate or other documentation of the death of the patient such as:
    - The Texas probate court or other state documents designating the administrator of the patient's estate.
  - Written statement from the Individual that he/she will not directly or indirectly identify the decedent in any report of the research or otherwise disclose the decedent's identity in any manner.
  - Certification from the Individual that the decedent's PHI will not be removed from BCM's premises.

# Research on Decedents' PHI (Cont.)

- The Privacy Compliance Officer will approve and sign the Request for Access to PHI for Research on Decedents and return the approved Form to the Individual.
- **Requests for PHI for Research on Decedents' PHI must be made using the Request for Access to Decedents' PHI for Research Form**

## Request for Access to Decedents' PHI for Research

I request to review health records for the following research purpose: Research on Decedents' PHI.

I am requesting access to or disclosure of information only of deceased individuals (*Please attach list of names*) and **I hereby represent that** (*Researcher must check all and attach the required documentation*):

- I will only access or use decedent's PHI solely for research;
- I will only access or use decedents' PHI that is necessary for the research study; and
- I am providing the following documentation of the death of the individuals whose information I am requesting:
  1. The patient's death certificate or other documentation of the death of the patient. (*Please attach*)
- I will not directly or indirectly identify a decedent in any report of the research or otherwise disclose the identity of the decedent in any manner
- I will not remove the PHI from BCM premises.

**Type of health information to which access is requested** (medical records, imaging studies, pathology information, lab information, etc.) and proposed review site:

- Electronic records: database(s) to be reviewed: \_\_\_\_\_
- Paper records: site of review (location and department): \_\_\_\_\_
- Imaging studies: site of review (location and department): \_\_\_\_\_
- Other: \_\_\_\_\_

Please describe your request below if BCM Office of Information Technology needs to generate the list for you. Otherwise, please attach the list of records you are requesting.

\_\_\_\_\_  
\_\_\_\_\_

If other individual(s) will be involved in the research related to the decedents' records requested, provide a signed memo identifying these individuals and their corresponding roles, and representing that all necessary training (CITI, HIPAA Privacy and Security) has been completed, and their signatures:

# Research on Decedents' PHI (Cont.)

If other individual(s) will be involved in the research related to the decedents' records requested, provide a signed memo identifying these individuals and their corresponding roles, and representing that all necessary training (CITI, HIPAA Privacy and Security) has been completed, and their signatures:

**I agree to the terms and conditions set forth above regarding access to Decedents' PHI for the research purpose indicated above. (Attach signature list if additional individuals are involved)**

\_\_\_\_\_  
*Signature*                      *Print Name*                      *Date*

\_\_\_\_\_  
*Signature*                      *Print Name*                      *Date*

I agree that the information I have requested will only be used for the research purpose stated in this Request Form and its accompanying documentation. I agree that I will use only the information necessary for the research purpose described. I will protect the confidentiality and security of this information while it is in my possession, and will destroy identifiers if required by accompanying documentation. I am aware that the data to which I have requested access is subject to HIPAA, Texas Privacy laws, and other legal and regulatory protections and that violation of privacy and confidentiality protections for this data may incur civil and criminal penalties. I understand and agree to comply with the obligations listed in this section as well as with all obligations described for the boxes I have checked above, and to inform all research team members of their responsibilities for compliance with these obligations..

\_\_\_\_\_  
Signature of Principal Investigator                      Date of Request                      Contact Information of Principal Investigator

\_\_\_\_\_  
Print Name                      \_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
Date Reviewed

Approved   
Denied

\_\_\_\_\_  
Signature of Privacy Compliance Officer

# Research on Decedents' PHI (Cont.)

- The Privacy Compliance Officer will approve and sign the Request for Access to PHI for Research on Decedents and return the approved Form to the Individual.
- Upon receipt of the signed Form from the Privacy Compliance Officer, the Individual must complete the Request for Access to PHI for Research which is available through ServiceNow and provide a copy of Form signed by the Privacy Compliance Officer.
- Uses or Disclosures of PHI for reviews that are Preparatory to Research are subject to:
  - The minimum necessary rules. See [BCM Policy No. 31.4.07, Uses & Disclosures of PHI: Minimum Necessary Standard](#)
  - Accounting of disclosures. See [BCM Policy No. 31.4.xx, Right to an Accounting of Disclosures](#)

# Limited Data Sets

- Limited Data Set (LDS) is PHI that excludes the direct identifiers (See List of Identifiers) of the Individual or of relatives, employers, or household members of the Individual, except for the following:
  - Dates of admission and/or discharge
  - Dates of birth
  - Dates of death (if applicable)
  - Five digit zip code or any other geographic subdivision (state, city, county, etc.)
- PHI constituting a LDS can only be Accessed, Used or Disclosed for Research and Public Health Activities pursuant to a written and fully executed Data Use Agreement (DUA) or Network and Database Agreement.
- A BAA is required if any PHI beyond a LDS is Accessed, Used or Disclosed for Health Care Operations. See BCM Policy No. 31.4.09, Uses & Disclosures of PHI: Business Associate Agreements.
- BCM Workforce Members can Use and/or Disclose a LDS, for Research and Public Health Activities **only** when a DUA has been fully executed by BCM and the other entity.

## Limited Data Sets (Cont.)

- A BCM Workforce Member seeking Access, Use or Disclosure of a LDS must send an email to [mta@bcm.edu](mailto:mta@bcm.edu) and provide a description of the PHI that will constitute the LDS.
- If, after review of the PHI requested, it is determined that it exceeds the elements of a LDS, a BAA is required.
- There can be no exchange of data until a DUA or a BAA is fully executed by BCM and the other Entity.



# Information Security & Compliance Program Goal

The goal of the BCM Information Security and Compliance Program is to protect **Confidential Information** by ensuring that only authorized persons use the information for its intended purposes.

This goal is achieved by implementing and overseeing security standards; administrative, physical and technical safeguards; organizational requirements; policies and procedures, documentation requirements.

All members of the BCM Community are required to maintain the security of **Confidential Information**, electronic or otherwise.

# BCM Security Compliance Requirements

BCM is a diverse institution. Our health care providers treat patients and teach students at each of BCM's affiliated institutions as well as at BCM's clinical departments, and outpatient clinics. BCM researchers also obtain confidential information for research purposes.

- **All BCM computing assets must be maintained securely to avoid risks of:**
  - Privacy violations
  - Identity theft
  - Compromised research protocols
  - Civil and/or criminal penalties
- References to BCM Information Security policies, procedures and guidelines are provided at [IT Policies and Guidelines](#)
- Security that is intentionally not maintained could result in a BCM employee's **loss of indemnification**. See [BCM Policies and Procedures for Legal Representation and Indemnification for Baylor Persons](#).
- Violation of the Security Compliance Program will result in **disciplinary action** up to and including termination from employment with BCM, or removal from educational programs.

# Security Standards for Computer Resources

**Information Security and Compliance provides security standards, including the HIPAA Security Standards Rule, for BCM computer resources.**

The BCM Information Security Officer oversees compliance with information security requirements.

**The BCM security standards require the following:**

- Provide for the confidentiality, integrity, and availability of all confidential information that is created, received, maintained or transmitted by BCM;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of confidential information;
- Protect against any reasonably anticipated uses or disclosure that are not permitted by BCM policy or regulatory requirements; and
- Provide for compliance with BCM security policies and regulatory requirements

# Security Standards for Electronic Media

BCM security standards apply to ALL electronic media (including personal devices) used for communicating and storing confidential information including but not limited to:



Desktop Computers



Tablets



Laptop Computers



Fax machines



Smartphones and PDAs



Flash drives



Copiers/printers



Internet / Web Storage



Telephone voice response / faxback systems

# HIPAA Security: Specification Categories

**BCM must address and meet the following six categories in order to comply with the Federal HIPAA security standards for electronic protected health information (ePHI).**

- 1. The HIPAA Security Standards General Rules** - provide the objective and scope for the HIPAA Security Standards Rule as a whole.
- 2. Administrative Safeguards** - documented formal practices to manage security measures to protect ePHI and manage the conduct of personnel who handle such information.
- 3. Physical Safeguards** - include the physical protection of computing assets from natural and environmental hazards and intrusion. This includes having appropriate access controls in place, data backup procedures, and disaster recovery plans.
- 4. Technical Safeguards** - include those mechanisms to guard ePHI integrity, confidentiality, and availability. Technical safeguards also include processes to prevent unauthorized access to ePHI that is transmitted over external networks (such as the Internet).
- 5. Organizational Requirements** - address business associates and requirements for group health plans.
- 6. Policies and Procedures and Documentation Requirements** - call for the implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Standards Rule.

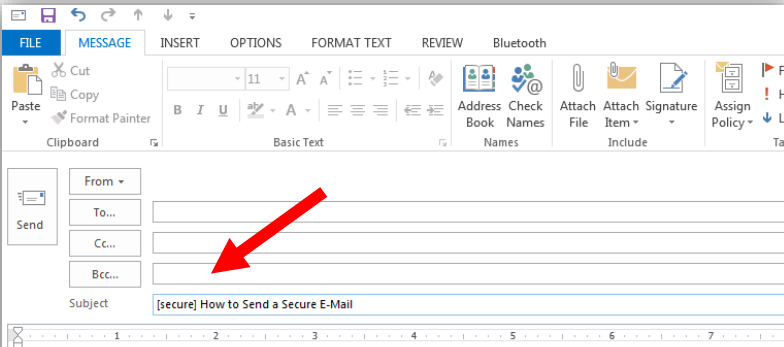
*All of the above requirements for a HIPAA-compliant security program to protect ePHI are established within the BCM HIPAA Program through BCM Information Security and Compliance.*

# Encrypted Messaging (e-mails)

All members of the BCM Community are responsible for the protection of confidential information through the following security requirements:

**Do use BCM encrypted secure messaging** (e-mail) and websites to guard against unauthorized access to confidential information being transmitted. Google, DropBox, and other public internet sites may not be secure or encrypted.

**DO NOT** use non-BCM or non-affiliate institution e-mail or websites for BCM business, particularly for **collecting or maintaining confidential information.**



The screenshot shows an email client window with a ribbon menu at the top (FILE, MESSAGE, INSERT, OPTIONS, FORMAT TEXT, REVIEW, Bluetooth). Below the ribbon are various toolbars for editing and sending. The main area shows the 'To...', 'Cc...', and 'Bcc...' fields, and the 'Subject' field. A red arrow points to the subject line, which contains the text '[secure] How to Send a Secure E-Mail'. Below the screenshot is a text box with the following content:

## How Do I Send a Secure E-mail?

To send an encrypted e-mail, simply enter the keyword tag **[secure]** (with the brackets) anywhere in the **subject line** of the message.

# Access to Baylor Property and Resources

Do ensure that **only authorized individuals have appropriate access** to confidential information and prevent those who are not authorized from obtaining access. Verify identities of individuals seeking access to confidential information and that they are authorized to access the information, consistent with BCM policies.

**Do NOT** allow **unauthorized individuals access to confidential information** or the computing devices that contain confidential information.

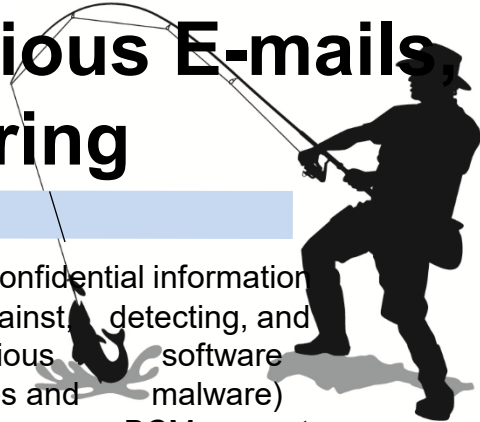
**DO use strong passwords** (at least 8 characters using upper/lower case, numbers and symbols with no well known words) and change at least every 90 days.

**Do NOT** share, give, or allow the use of **your BCM password** under any circumstances. Make sure your computer is locked every time you leave it.

**DO limit the physical access** to confidential information and the facility or facilities in which information is housed, while ensuring that properly authorized access is allowed. Specify which computing assets can access confidential information and physically safeguard them. For example, laptops must be encrypted as well as kept in a locked area when not in use.

**Do NOT** allow **unauthorized individuals access to BCM or affiliate institution facilities**. Authorized individuals have badge passes.

# Malicious E-mails Spearing



**DO protect** confidential information by guarding against, detecting, and reporting malicious software (such as viruses and malware) and attempts to access BCM computer assets and information through malicious e-mails. Report malicious software and attempts to access to your supervisor and the BCM Information Security Officer. Use only approved software on BCM computer assets.

**DO NOT click on links** from correspondence you were not expecting or enter your BCM login or password due to an e-mail prompt, even if the e-mail appears to be from BCM. **REMEMBER, BCM WILL NEVER ASK YOU FOR YOUR USER NAME AND PASSWORD.**

# Phishing,

## Quick tips for spotting a malicious e-mail:

- The e-mail subject line or body **is out of character**, even if from a BCM person.
  - Do not click on links or attachments you are not expecting. Confirm with sender.
- You are being urged to log into an account by **clicking a link**. Or, you are being threatened if you don't act quickly (e.g., "you will be locked out").
  - Scroll your mouse (without clicking) over the link in an e-mail to reveal its real address. If it looks strange (e.g., random numbers or letters or unfamiliar web address) delete the e-mail immediately and contact the IT Help Desk at 713-798-7618 or [it-support@bcm.edu](mailto:it-support@bcm.edu)
- You are **being offered anti-virus** intervention.
  - Beware of spam e-mails and social network messages warning of fictional security threats with anti-virus software attached. Delete the e-mail immediately and contact the IT Help Desk at 713-798-7618 or [it-support@bcm.edu](mailto:it-support@bcm.edu)



# Follow Policies, Protect Confidential Information

**DO** comply with, create, maintain, make available, implement, **follow, and enforce policies and procedures** within your area that comply with BCM security standards. Do encrypt authorized confidential information maintained on BCM computing assets.

**DO NOT violate BCM or affiliate organizations policies**, procedures, guidelines, reminders, or notifications

**DO NOT collect confidential information without authorization** of the affiliate institution or individual whose information is being used.

**DO encrypt confidential information** collected or maintained on computing assets (flash drives, laptops, Smartphones, cameras, and other computing assets). The computing assets that collect or maintain ePHI must be encrypted. Contact the IT Help Desk at 713-798-7618 or [it-support@bcm.edu](mailto:it-support@bcm.edu) for BCM-owned computing assets encryption assistance.

**DO NOT** collect or maintain **confidential information with unsecured electronic devices** (non-encrypted or weak password protection).

**DO NOT** use **personal computing assets** to collect or maintain BCM or affiliate institutions' **confidential information**.

**DO protect confidential information** from improper alteration or destruction.

**DO NOT intentionally destroy or damage** BCM computing assets.

**DO** prepare for an emergency, such as natural disaster, fire, vandalism or system failure by **creating and maintaining retrievable backup copies and confidential information**, and make them available during the emergency. Periodically evaluate security specifications in response to environmental or operational changes. IT backs up information maintained in IT managed information systems (files, folders, etc.).

**DO NOT remove confidential information from BCM** without authorization or the appropriate security measures in place.

# Acceptable Use Standard

**DO** observe **BCM's Acceptable Use Policy and all IT Security Policies** for use and access of all BCM computers, information systems and **network** resources

**DO NOT** use BCM computing assets for **personal business** in a manner that would subject you or BCM to any legal action or in an improper or inappropriate manner.

**DO NOT** use BCM computing assets to transmit, display or print material that contains profane language, panders to bigotry, racism or sexism, or promotes or facilitates any form of **illegal discrimination**.

**DO NOT** copy, duplicate, install, electronically forward, distribute or use **copyrighted works** (including but not limited to software, images, data, sounds and multimedia works) which infringe on the copyright of another.

**IF YOU DON'T KNOW, ASK.**

**Monitor and report unauthorized attempts to access confidential information and report the attempts to your supervisor, and the BCM Information Security Officer Jeff Pounds, [jpounds@bcm.edu](mailto:jpounds@bcm.edu).**

# Reporting Violations

- All BCM workforce members are required to report any suspected breaches of privacy and/or security of PHI or other information to the Privacy and/or Security Officers with Compliance and Audit Services as soon as possible. If a BCM workforce member does not report an alleged violation to his/her supervisor, management, faculty member, peer or physician in instances where they believe violations of the BCM Code of Conduct, policies, standards, ethics, or laws have occurred, disciplinary action may be imposed.
- Policy can be found here:  
<https://intouch.bcm.edu/sites/compliance-and-audit-services/SitePageModern/2662/integrity-hotline>
- BCM Policy and Procedure Manual can be found here:  
<https://intranet.bcm.edu/index.cfm?fuseaction=Policies.Policies&are a=31>

# Reporting Violations

HIPAA Privacy Compliance  
[privacycompliance@bcm.edu](mailto:privacycompliance@bcm.edu)

**Jeffrey S. Pounds**  
Information Security Officer  
Phone: 713-798-7618  
[jpounds@bcm.edu](mailto:jpounds@bcm.edu)

**HIPAA Privacy Incident Report Form:** BCM Intranet <Admin Offices <Compliance and Audit <HIPAA Compliance Program <Forms

## Integrity Hotline

- Call 855-764-729 (toll free); OR
- Submit a report online at:

BCM Intranet < Admin Offices <Compliance and Audit <Integrity Hotline



# Questions

