POM ACO
TRANSFORMING HEALTH CARE TOGETHER

Health Data Privacy & Security Rules “The Basics”

HIPAA Learning Module

MICHIGAN MEDICINE UNIVERSITY OF MICHIGAN · OLYMPIA MEDICAL · IHA · UNITED PHYSICIANS Advancing Physician Performance · aH ANSWER HEALTH · OSP POWERED BY ADMINISTRATIVE NETWORK · WEXFORD/CRAWFORD PHYSICIAN HOSPITAL ORGANIZATION · hvpa Huron Valley Physicians Association P.C. · MidMichigan Collaborative Care Organization

Our Commitment to Privacy

HIPAA Learning Module: The Basics

- The HIPAA Privacy and Security Rules protect individuals' medical records and other personal health information.
- POM ACO is committed to protecting the privacy and integrity of beneficiary health information.
- Protecting beneficiary Health Information is the responsibility of all of us.

Learning Objectives

HIPAA Learning Module: The Basics

- Key things for you to know:

  ✓Just Ask! Check with your compliance office or the POM ACO compliance team whenever you have a question or concern.

  ✓HIPAA key terms & general rules you can apply.

  ✓Your role in protecting patient information.

POM ACO
TRANSFORMING HEALTH CARE TOGETHER

Key Term: Protected Health Information (PHI)

- PHI is health information about a beneficiary created or received by health care providers and health plans.

- PHI is information that:
  - Identifies a beneficiary or can be used to identify a beneficiary.
  - Concerns a beneficiary’s past, present or future treatment and/or payment of services.
  - Involves any form (written, verbal, electronic).

Key Term: Protected Health Information (PHI)

- PHI includes one or more of these identifiers:
  - Name, includes initials
  - Address, Zip Codes
  - All Dates
  - Telephone & Fax Numbers
  - Email Addresses
  - Social Security Numbers
  - Medical Record Numbers
  - Health Plan Numbers
  - License Numbers
  - Vehicle Identification Numbers
  - Account Numbers
  - Biometric Identifiers
  - Full Face Photos
  - Any unique identifying number, characteristic, code

PHI is health information that can lead to the identity of an individual or when the contents of the information can be used to make a reasonable assumption as to the individual's identity.

Key Term: Covered Entity

HIPAA privacy & security rules apply to ACOs just like they do to covered entities.

- ACO Participating hospitals and physician practices are HIPAA covered entities because they provide care to CMS beneficiaries and bill CMS for that care.
- POM ACO is not a covered entity because it neither provides care or bills for care.
- POM ACO is bound by law to comply with HIPAA:
  - Federal regulations governing ACOs require it.
  - POM ACO is considered a business associate to its participating covered entities, like Michigan Medicine.

Key Term: Business Associate

- Individuals or organizations that access/use a covered entity's (CE) protected health information to carry out health care operations on behalf of the CE.

- Health care operations are things like conducting quality assessments and improvement activities, perform care coordination and conduct population-based activities.

- CEs and their Business Associates enter into Business Associate Agreements (BAA) - a signed agreement promising to keep a CE's PHI confidential and protected in accordance with HIPAA.

Key Term: Minimum Necessary

- **Minimum Necessary Rule**: Generally, the amount of PHI used, shared, accessed or requested must be limited to only what is needed. Workers should access or use only the PHI necessary to carry out their job responsibilities.
- ACOs may only have access to the minimum amount of data to carry out its health care operational objectives.

For Example:

- ACO data analysts should not use or disclose a beneficiary's health or billing data for troubleshooting purposes, unless absolutely necessary; in which case, the analysts must only use or disclose only what is minimally needed to accomplish their work objective and must only use secure (HIPAA compliant) transmission methods.

Contact your IT service department to learn what are approved data transmission methods. Only use these methods.

Test Yourself

Question:

If you have a document that contains a beneficiary’s initials and health plan number, does your document contain PHI?

Test Yourself

Answer: Yes

Initials and health plan numbers can be used to identify individuals. It does not matter that the full name is not included.

PHI is any information that is received, sent or stored by a provider or health insurance plan:

- That identifies a beneficiary or can be used to identify a beneficiary.

In other words: PHI is any health information that can lead to the identity of the individual or the contents of the information can be used to make a reasonable assumption as to the individual's identity.

Test Yourself

Take Away:

Do not use beneficiary identifiers if you do not need to do.

If the use of identifiers cannot be avoided, then only use those identifiers that you <u>minimally need and nothing more</u>.

Key Term: Incidental Disclosure

Some disclosures are not completely avoidable. These are permitted under HIPAA and are called "Incidental Disclosures"

- HIPAA requires reasonable steps to be taken to minimize incidental disclosures such as:
  - Redact/Remove PHI from e-mail and screen shots when conducting GPRO troubleshooting activities or other activities involving sensitive information.
  - Speaking in soft tones when discussing PHI in open areas, etc.
  - Not including any PHI when it is not necessary your work.

In all cases: only use the minimum necessary to minimize incidental disclosures.

Key Term: "Highly Confidential" Information

- Federal and Michigan State Law provide additional protections beyond HIPAA in some cases for data that is about:
  - Mental Health and Substance Abuse
  - HIV/AIDS Testing or Treatment
  - Genetic Tests/Information
  - Certain communicable diseases (e.g., sexually transmitted disease, hepatitis, etc.)
  - Certain diagnostic and treatment services rendered to minors like pregnancy and prenatal care
  - Discuss with your supervisor about special precautions to protect highly confidential information.

If you have questions about handling highly confidential information, ask your compliance officer.

Test Yourself

Question:

You are a nurse asking a newly admitted patient a number of questions as part of the admission process. You see that the patient is HIV positive. Would it be appropriate for you to discuss the beneficiary’s HIV status in front of the patient’s family member?

Test Yourself

Answer: No.

Because HIV status is highly confidential information, it is subject to greater protections beyond HIPAA.

In this scenario, you should not discuss any highly confidential information in front of the patient’s family member without patient’s permission. Instead, require that the family member to leave the room before proceeding with gathering your information to complete your admission paperwork.

Accessing Electronic PHI

Use and Disclosure of Electronic PHI:

- Use your electronic access to information systems only to perform your job-related duties and only access PHI on a need-to-know basis.
- Inappropriate access, use, or disclosure of a beneficiaries PHI can lead to disciplinary action, up to and including termination.

Test Yourself

Question:

Would it be permissible for you to look up a beneficiary's address to contact them to send them a get well card?

Test Yourself

Answer: No

You cannot access beneficiary information for purposes that are not job-related.

Accessing the electronic medical record or other data systems containing beneficiary health information for purposes other than to complete your job responsibilities is not permitted.

Inappropriate access to beneficiary information can lead to disciplinary action.

Information Security – Protecting PHI

HIPAA Learning Module: Basic

POM ACO

TRANSFORMING HEALTH CARE TOGETHER

Information Security – Protecting PHI

- Use difficult to break passwords.
- Never share your password with another person.
- Log off from all electronic record applications before walking away from the computer.
- Secure all electronic records using encryption – Call IT support to set up secure electronic systems.
- All portable electronic devices used for ACO business such as laptop computers, flash/thumb drives, electronic tablets, etc. must be encrypted.
- Never send PHI using an unsecured transmission method, e.g, comcast, yahoo, g-mail.

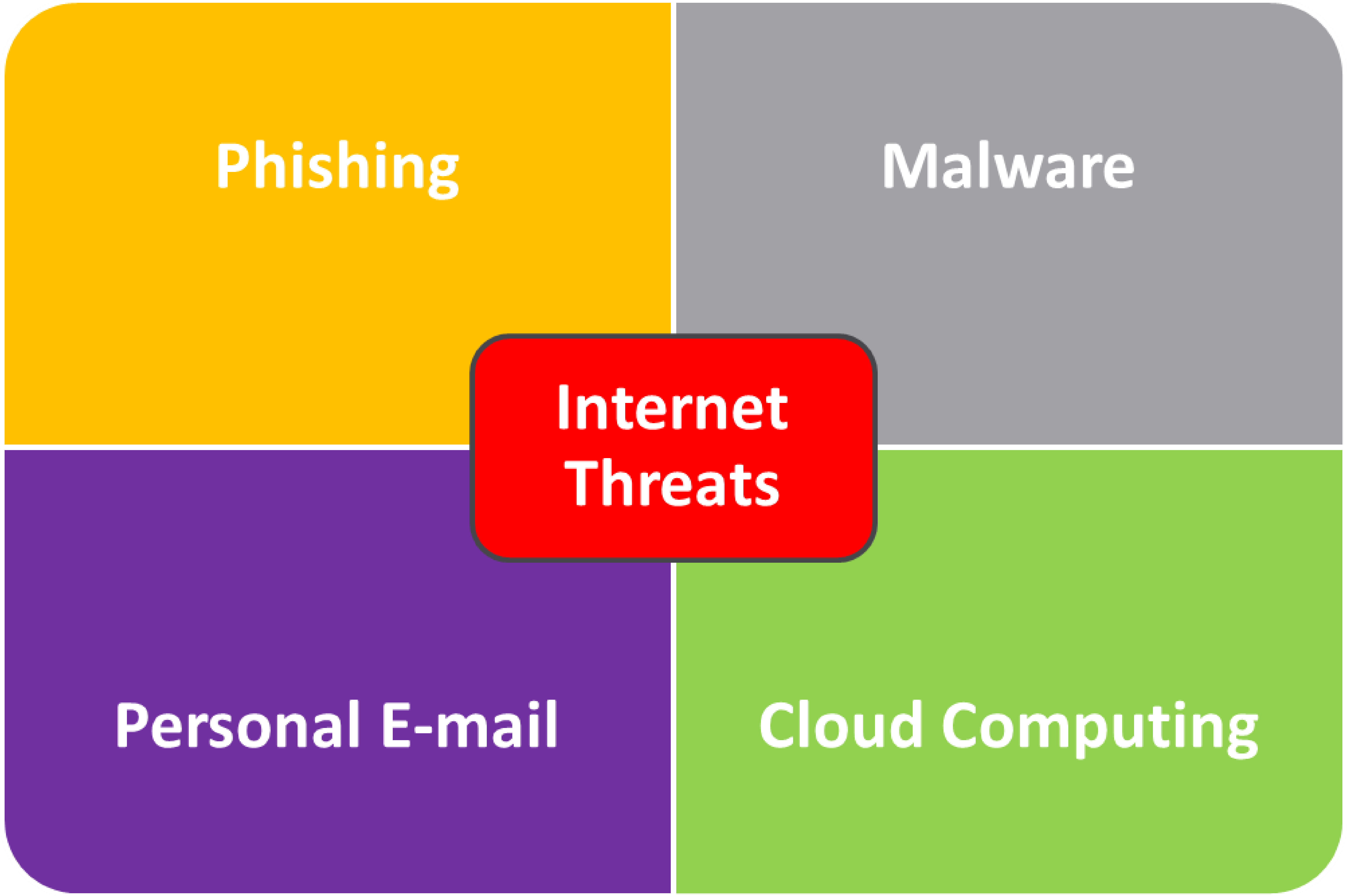
Immediately report to your compliance Officer if CMS beneficiary PHI is inappropriately used or disclosed.

Strong Passwords

In addition to encryption, a “strong” password is an important way to protect confidential information stored electronically

- Use at least 8 characters (9 or more is ideal), unless limited by system capabilities
- Use at least 3 of the following character types:
  - Lowercase and uppercase letters
  - numbers
  - symbols (@, %, $, &, etc.)
  - punctuation marks (?, !, etc.)
- Do not use names, identifiers, simple phrases or words in any language ("password", "michigan", your user ID, "hello2u", etc.)
- Do not use sequences of characters or keys ("123456", "abcdef", "qwerty", etc.)
- Use different passwords on different systems so if one password is lost or stolen, there is no risk to the other systems.

Internet Threats to watch out for



Phishing

Malware

Internet Threats

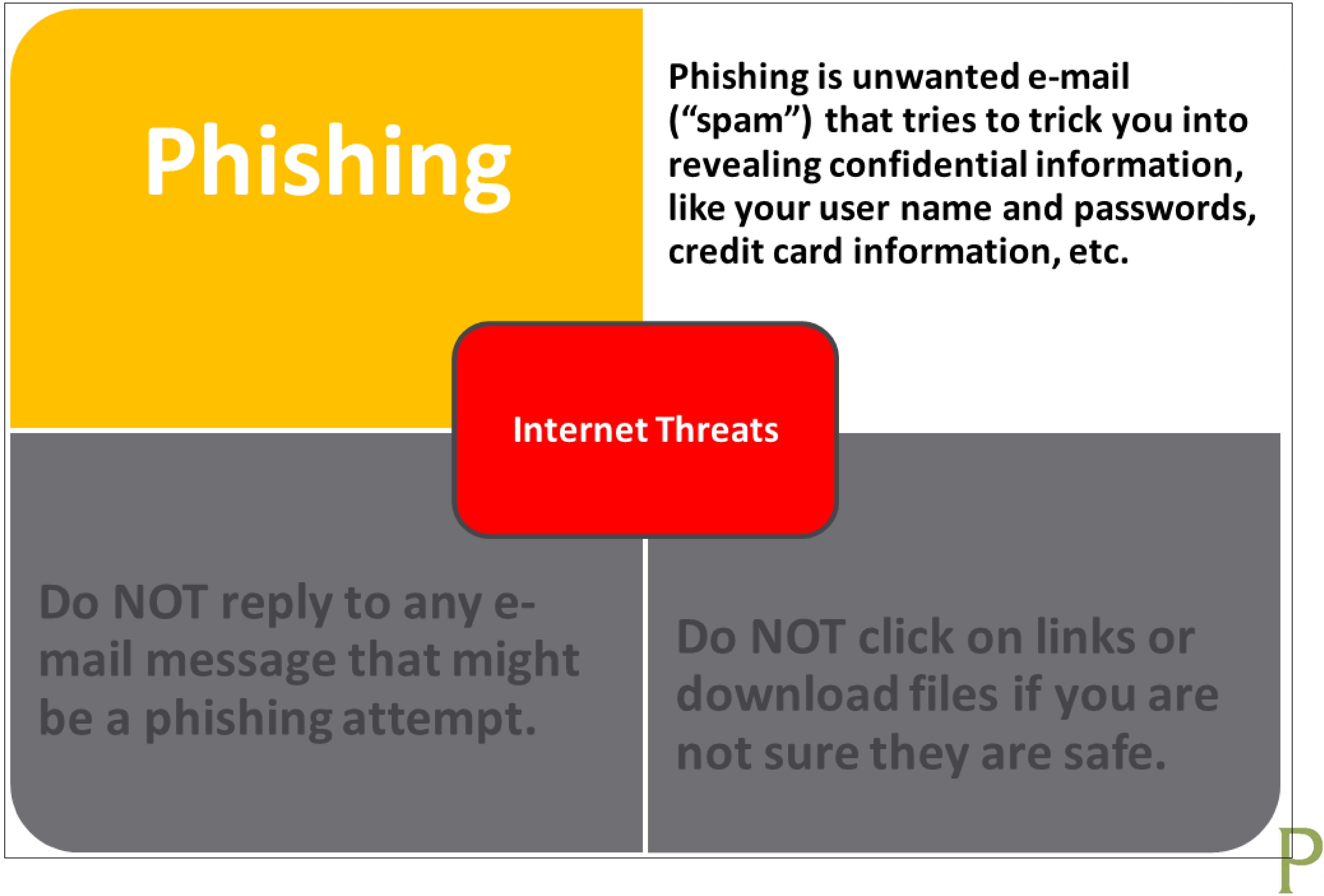
Personal E-mail

Cloud Computing

POM ACO

TRANSFORMING HEALTH CARE TOGETHER

Internet Threats - Phishing



Phishing

Phishing is unwanted e-mail ("spam") that tries to trick you into revealing confidential information, like your user name and passwords, credit card information, etc.

Internet Threats

Do NOT reply to any e-mail message that might be a phishing attempt.

Do NOT click on links or download files if you are not sure they are safe.

Internet Threats: Malware

Malware is software designed to harm your computer. Malware gets into your computer through e-mail attachments, compromised websites, etc.

Malware

Internet Threats

Examples: Computer virus, worms and spyware. It can destroy your data and cause inappropriate access to or disclosure of sensitive information such as PHI.

Malware is blocked through an up-to-date antivirus software program and antispyware scanning program. Contact your IT Support for help.

Internet Threats: Cloud Computing

Cloud computing gives access to computer files and programs over the internet, and may include backing up or synchronizing those files with a cloud service pr

Gmail, Google Calendar, Google Docs, etc. are examples of “Cloud Services”

Internet Threats

Cloud Computing

NEVER store PHI or other sensitive information on public cloud services*

NOTE: Use of Cloud Service Provider(s) requires special contracts and information security specifications.

Contact POM ACO Executive team before using any cloud service provider.

Internet Threats: Personal Email

Only use approved electronic data transmission methods – check with you IT Service provider

E-mail sent outside your institution must be encrypted. Do not use public accounts such as:
"@gmail.com"
"@yahoo.com"
"@comcast.com"

Internet Threats

Personal E-mail

Do NOT transmit PHI or other sensitive information to or from your personal email

E-mailing PHI is Not Allowed

- **E-mail Users:**
  - E-mail to e-mail transmission between participating sites is not considered secure. (This includes email to a “umich.edu” address or to a hotmail®, yahoo®, comcast®, or other type of business or personal e-mail address)
- **POM ACO requires:**
  - All e-mail transmissions containing CMS beneficiary data must be encrypted, even if no PHI is present.

Check with your compliance officer and/or your IT service provider for determining appropriate encryption methods.

Encryption is key

- PHI must be encrypted at all times – at rest and in-motion.
- Proper Encryption makes data on computers and other electronic devices unreadable. Users must have an “encryption key” to “unlock” the encryption to access the data.

Check with your compliance officer and/or your IT service provider for determining appropriate encryption methods.

Test Yourself

Which of the following is a strong password?

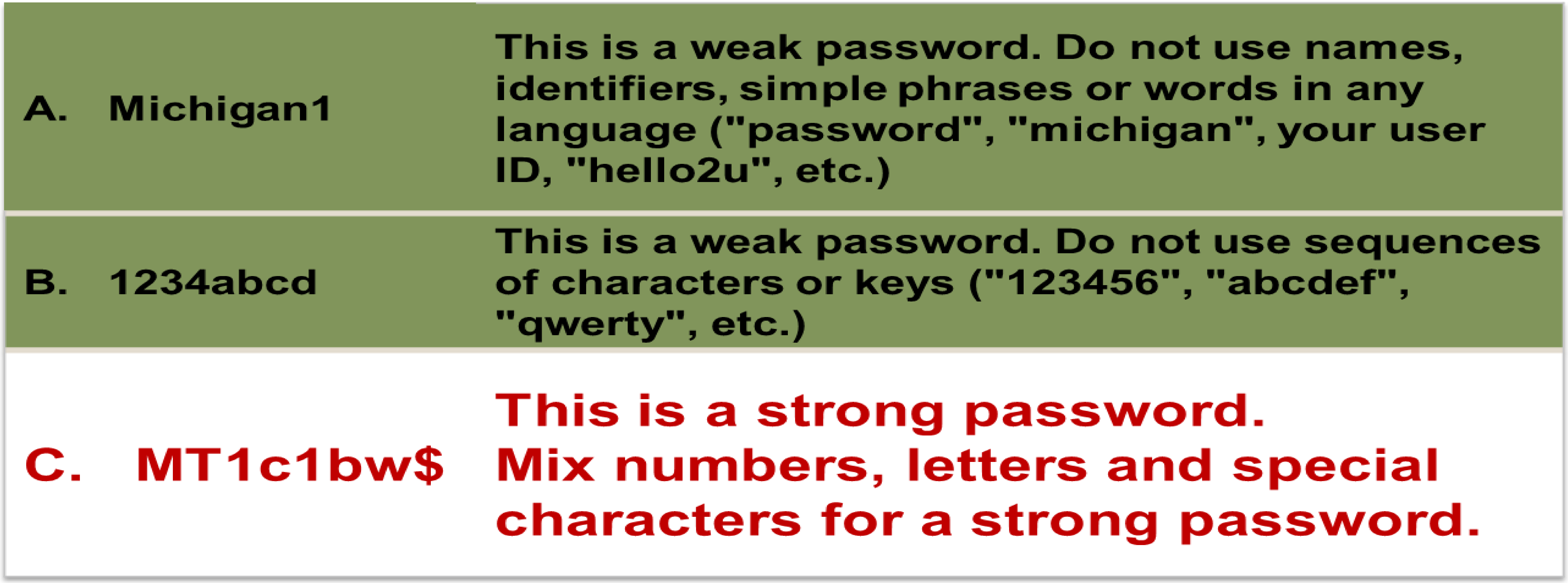
A. Michigan1

B. 1234abcd

C. MT1c1bw$

Test Yourself

Answer: C



A.	Michigan1	This is a weak password. Do not use names, identifiers, simple phrases or words in any language ("password", "michigan", your user ID, "hello2u", etc.)
B.	1234abcd	This is a weak password. Do not use sequences of characters or keys ("123456", "abcdef", "qwerty", etc.)
C.	MT1c1bw$	This is a strong password. Mix numbers, letters and special characters for a strong password.

Breach and Breach Notification Rules

Security incident Notification Rules

HIPAA Learning Module: Basic

POM ACO

TRANSFORMING HEALTH CARE TOGETHER

CMS Data Use Agreement (DUA) Governs Notification and Reporting Requirements

CMS Data Agreement Applies to all sites receiving CMS claims data:

- Outlines acceptable uses & disclosures CMS Claims data
- Requires compliance to HIPAA Privacy & Security Rules
  - HIPAA requires all HIPAA breaches to be reported to the Office for Civil Rights
- Outlines data recipient obligations:
  - Protect privacy of subject individuals
  - Appropriately technical, physical and administrative controls to protect the data.
- Requires all **suspected** data security incidents to be reported to CMS.

Security incident reporting is subject to tight time frames
Immediately report all concerns to your compliance officer!
Reports MUST be received within 30-minutes of discovery.

All violations are PRESUMED a "BREACH"

All Privacy & Security incidents must be analyzed for a HIPAA violations.

Federal law considers all HIPAA violations to be a Breach.

To overcome this presumption of a Breach your compliance office must conduct a 4-prong test.

REPORT ALL SUSPECTED PRIVACY OR SECURITY CONCERNS to POM ACO within 30-minutes.

4-prong test:

1. Nature and extent of information involved, including the types of identifiers and risk of re-identification
2. Unauthorized person who used the PHI or to whom it was disclosed
3. Whether the PHI was actually acquired or viewed
4. Extent to which risk to the PHI has been mitigated

POM ACO

TRANSFORMING HEALTH CARE TOGETHER

HIPAA: Notifications

- If Breach, Written Notice Must Be Provided
  - All patients whose information is involved
  - Federal Department of Health & Human Services, Office for Civil Rights
  - Media (If >500 patients from single jurisdiction)
  - If patients are research subjects, IRB Director reviews/gives input on draft notice letter

- Discovery Date Starts Clock for Notice Provision
  - HIPAA Requirement vs. Our Experience
  - Unreasonable delays (e.g., waiting while someone is on vacation)

POM ACO - HIPAA Breach Notifications

- When there is a Breach, the Covered Entity must provide written “Breach” notice:
  - To Every Individual Affected
  - To Federal Government - Department of Health & Human Services/Office for Civil Rights (“OCR”)
  - To Media – If >500 individuals residing in single state or “jurisdiction” (e.g., SE Michigan)

Fines and Penalties

- **Civil Fines Up to $1.5 million** per HIPAA violation per year (prior max was $25,000/violation/year)

- Criminal fines: $250,000/up to 10 years imprisonment, **criminal penalties expanded to individuals.** NOTE: Individuals (This means You!) can be subject to criminal prosecution, fines and imprisonment

Reporting a POM ACO Concern

- POM ACO Related Concerns:
  - Calling 1-734-232-1482
  - Emailing tdesjard@umich.edu
  - On-line at www.reportlineweb.com/pomaco

Questions?

- For questions about HIPAA:
  - http://www.med.umich.edu/u/compliance/area/privacy/index.htm

- For more information:
  - http://www.hhs.gov/ocr/privacy/
  - http://www.cms.hhs.gov/HIPAAGenInfo/