HIPAA Privacy and Security

April 13th, 2022

CHILDREN'S & WOMEN'S HOSPITAL | MITCHELL CANCER INSTITUTE | PHYSICIANS GROUP | UNIVERSITY HOSPITAL | COLLEGE OF MEDICINE

USA HEALTH

Agenda

- Purpose and Background of HIPAA Rules
- What is PHI
- Who must comply with HIPAA Rules
- How Can PHI be Used and Disclosed For Research
- Business Associates
- Security Best Practices

USA HEALTH

Purpose and Background of HIPAA Rules Related to Research

- Establishes the conditions under which protected health information (PHI) may be used or disclosed by covered entities for research purposes.

- Defines the means by which individuals will be informed of uses and disclosures of their PHI for research purposes and their rights to access information about them held by covered entities.

USA HEALTH

What is PHI

Any information, including demographic data, that identifies or can be used to identify a patient, that relates to the patient's past, present, or future physical or mental health or condition, the provision of health care to the individual, or the past, present or future payment for the provision of health care to the individual.

USA HEALTH

What is PHI? (continued)

Protected health information includes all **individually identifiable health information.**

USA HEALTH

Who Must Comply with HIPAA

- Health care providers who transmit personally identifiable health information in electronic format in connection with a HIPAA covered electronic transaction;
- Health plans;
- Health care clearinghouses; and
- Business Associates of covered entities.

USA HEALTH

HIPAA Applicability for Research

- HIPAA Applies only to Covered Entities
- Researchers are covered entities if they are also health care providers
- Affects researchers because it affects their access to information
- To gain access for research purposes to PHI created or maintained by a covered entity the researcher may have to provide supporting documentation on which the covered entity may rely in meeting compliance with HIPAA

USA HEALTH

De-identifying PHI

- HIPAA lists 18 identifiers that must be removed before PHI can be shared without the patient's authorization. If all 18 are removed from the data, then it is considered de-identified or anonymized and not subject to HIPAA.
- The following 18 identifiers must be removed for de-identification.

USA HEALTH

HIPAA Identifiers

- Names
- Geographic subdivisions smaller than a state
- Elements of dates (except year)
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers/serial numbers
- Device identifiers and serial numbers
- Biometric identifiers
- Web URL's
- Internet protocol (IP) address
- Full-face photographic images
- **Any other unique identifier**

USA HEALTH

How the Rule Works

Covered entities are permitted to use and disclose PHI for research with the individual's authorization or without the individual's authorization under limited circumstances which HIPAA defines.

USA HEALTH

Authorization for Research Uses and Disclosures

- The basic rule is that research is not part of “treatment’, “payment” or “healthcare operations”, therefore the researcher must obtain a HIPAA authorization prior to receiving any PHI for use in research.

Exceptions to this rule:

- IRB has waived or altered the requirement for HIPAA authorization
- Use of a limited data set and the researcher has signed a HIPAA Data Use Agreement
- Reviews preparatory to research by staff of covered component
- The PHI has been de-identified prior to its use or disclosure for research
- Research involving a decedent’s information

USA HEALTH

What is the difference between HIPAA "Authorization" and informed consent?

- Informed consent is required under federal research regulations for the protection of human subjects.
  - HIPAA, a different regulation, separately requires that patients give written Authorization before a CE may use or disclose patient PHI for research.
- There are different requirements for the content of informed consent and HIPAA Authorization; however both may be combined in one form.
- IRB may waive consent and Authorization if the research meets all of the waiver criteria established by each of the applicable regulations.

USA HEALTH

Is IRB approval necessary if only de-identified information will be used in research?

- If the research involves only the analysis of pre-existing data that has been fully de-identified to the HIPAA standard, you do not need to submit to IRB because such research involves neither PHI not and identifiable human subject.
- If, however, de-identified data must be extracted from medical records or other identifiable sources for use in research or to create a de-identified database for future research, you must submit an application to IRB.

USA HEALTH

Data Use Agreement

- Means by which covered entities obtain satisfactory assurances that the recipient of the limited data will use or disclose the PHI in the data set only for specified purposes.
- If a covered entity is the recipient of a limited data set and violates the data use agreement it is deemed to have violated HIPAA
- DUA must be in place even if person requesting the limited data set is a member of the covered entity's workforce
- DUA must contain specific HIPAA provisions

USA HEALTH

Reviews Preparatory to Research

Researchers that are workforce members may access PHI for recruitment of potential participants in a study when the researcher makes representation that the use or disclosure of PHI is:

- Solely to prepare a research protocol
- The researcher will not remove the PHI from the premises, and
- The use or disclosure is necessary for research purposes

USA HEALTH

Research on Decedents

PHI associated with a deceased person may be used or disclosed for research purposes without an authorization. A covered component may rely on a researcher's oral or written representation that:

- The use or disclosure of the PHI is solely for research on the PHI of a decedent;
- That the PHI sought is necessary for the research; and
- At the request of the covered entity that documentation of the death of the affected individuals be provided.

USA HEALTH

Minimum Necessary Restriction

Covered entities are required to limit PHI used, disclosed, or requested to the minimum amount reasonably necessary to achieve the purpose for which disclosure is sought.

Exceptions

- Uses and disclosures made with an individual's authorization
- Disclosure to or request by a health care provider for treatment
- Disclosure to the individual
- Use and disclosure required by law
- Disclosures to HHS for purposes of determining HIPAA compliance

USA HEALTH

Access to PHI

HIPAA guarantees individuals access to PHI within “designated record set”

- Research records may be part of a designated record set if the records are medically related or are used to make decisions about research participants and are maintained by the covered entity
- Right of access can be temporarily suspended while research is in progress if individual agrees, during consent

USA HEALTH

Where should PHI be stored for research

- In the medical record system(s)
- University of South Alabama's Google space (non-commercial accounts)
- USA Health's Microsoft 365 space (non-commercial accounts)

USA HEALTH

Business Associates

USA HEALTH

Who is considered a Business Associate?

A “business associate” is **a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to**, a covered entity.

USA Health is considered a covered entity under the HIPAA regulation.

USA HEALTH

Are You Working with a Business Associate?

Ask yourself the following to determine if you are working with a business associate:

Is the service provider/vendor a member of the University of South Alabama/USA Health workforce?

- If Yes – they are not a business associate.
- If No – they are a business associate.

USA HEALTH

Are You Working with a Business Associate?

Ask yourself the following to determine if you are working with a business associate:

Does this service provider/vendor create, receive, transmit and/or maintain (includes cloud storage service) PHI, on behalf of the University of South Alabama/USA Health, as part of the services provided?

- If Yes – they are a business associate.
- If No – they are not a business associate.

USA HEALTH

Are You Working with a Business Associate?

Ask yourself the following to determine if you are working with a business associate:

Is the PHI being disclosed to a healthcare provider for treatment purposes (e.g., primary/referring physician, contract physicians or specialists, contract nursing staff, contract rehab staff, ambulance, home health, dentist, etc.)?

- If Yes – they are not a business associate.
- If No – they are a business associate.

USA HEALTH

What is a Business Associate Agreement (BAA)?

A business associate agreement is a written contract, required by the HIPAA regulation, between the business associate and the covered entity (or other business associates) with specified language regarding the use, disclosure, and protection of PHI.

USA HEALTH

When is a BAA required?

A BAA is required **any time** you are entering into a contract with a service provider/vendor who meets the criteria of a business associate. If a contract is being renewed and a BAA is already on file, a new BAA is not typically* required.

Note, if there is a breach of PHI and a business associate is involved, one of the things the HHS/OCR is going to require is a copy of or an attestation that the BAA was fully-executed between USA and the service provider/vendor **prior to the breach occurring**.

**In some instances, the BAA is out of date and new version needs to be reviewed and executed.*

USA HEALTH

Who is Responsible for Obtaining the BAA?

The department contact who is entering into the contract with the service provider/vendor is responsible for obtaining the BAA.

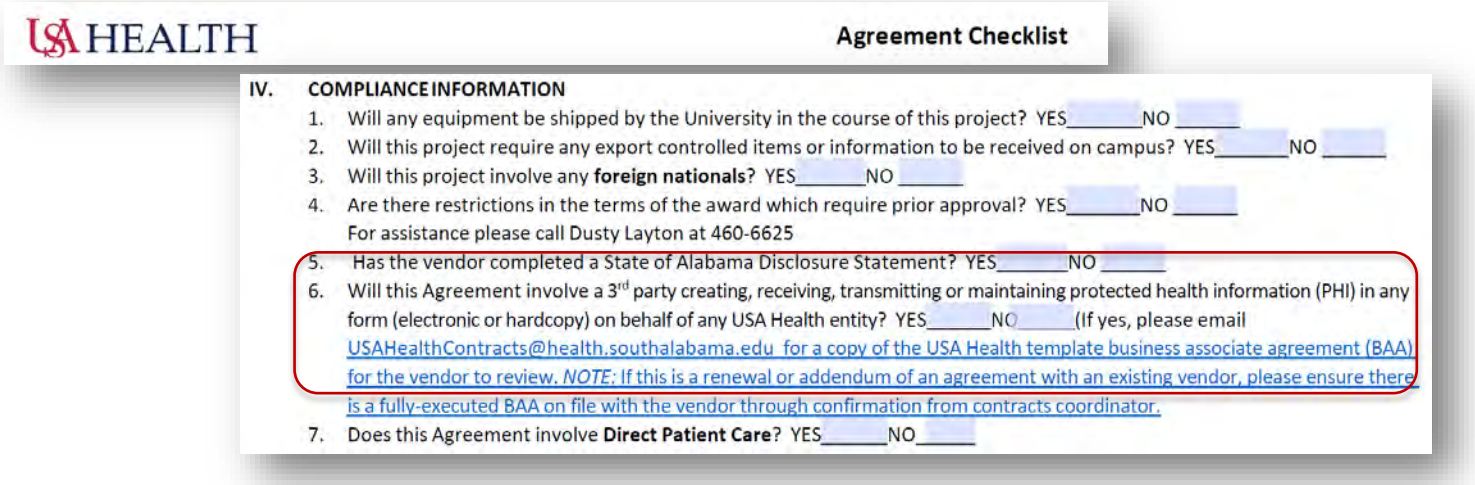
For service providers/vendors who may have worked with USA Health previously the department should contact the USA Health Contract Coordinator (by emailing: USAHealthcontracts@health.southalabama.edu/) or the Office of HIPAA Compliance to ensure BAA is already on file. When in doubt, please ask.

Remember, the BAA is considered a contract and can only be signed by the designated contracts officer.

USA HEALTH

How Does One Obtain a BAA?

The USA Health department contact should indicate on the Agreement Checklist that the service provider/vendor will be accessing, using and/or disclosing PHI. Once received by the Contracts Coordinator the need for a BAA will be reviewed and acted upon.



USA HEALTH **Agreement Checklist**

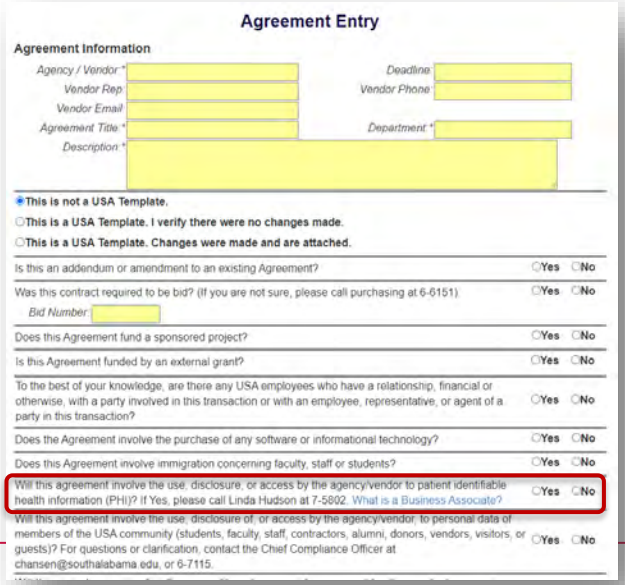
IV. COMPLIANCE INFORMATION

1. Will any equipment be shipped by the University in the course of this project? YES_____NO _____
2. Will this project require any export controlled items or information to be received on campus? YES_____NO _____
3. Will this project involve any **foreign nationals**? YES_____NO _____
4. Are there restrictions in the terms of the award which require prior approval? YES_____NO _____
   For assistance please call Dusty Layton at 460-6625
5. Has the vendor completed a State of Alabama Disclosure Statement? YES_____NO _____
6. Will this Agreement involve a 3rd party creating, receiving, transmitting or maintaining protected health information (PHI) in any form (electronic or hardcopy) on behalf of any USA Health entity? YES_____NO_____(If yes, please email USAHealthContracts@health.southalabama.edu for a copy of the USA Health template business associate agreement (BAA) for the vendor to review. *NOTE*: If this is a renewal or addendum of an agreement with an existing vendor, please ensure there is a fully-executed BAA on file with the vendor through confirmation from contracts coordinator.
7. Does this Agreement involve **Direct Patient Care**? YES_____NO_____

USA HEALTH

How Does One Obtain a BAA?

The University of South Alabama (campus) department contact should indicate, in the Agreement Tracking System, that the service provider/vendor will be accessing, using and/or disclosing PHI.



Agreement Entry

Agreement Information

Agency / Vendor * | Deadline
Vendor Rep | Vendor Phone
Vendor Email
Agreement Title: * | Department *
Description: *

- This is not a USA Template.
- This is a USA Template. I verify there were no changes made.
- This is a USA Template. Changes were made and are attached.

Is this an addendum or amendment to an existing Agreement?	Yes No
Was this contract required to be bid? (If you are not sure, please call purchasing at 6-6151)	Yes No
Bid Number:	
Does this Agreement fund a sponsored project?	Yes No
Is this Agreement funded by an external grant?	Yes No
To the best of your knowledge, are there any USA employees who have a relationship, financial or otherwise, with a party involved in this transaction or with an employee, representative, or agent of a party in this transaction?	Yes No
Does the Agreement involve the purchase of any software or informational technology?	Yes No
Does this Agreement involve immigration concerning faculty, staff or students?	Yes No
Will this agreement involve the use, disclosure, or access by the agency/vendor to patient identifiable health information (PHI)? If Yes, please call Linda Hudson at 7-5802. What is a Business Associate?	Yes No
Will this agreement involve the use, disclosure of, or access by the agency/vendor, to personal data of members of the USA community (students, faculty, staff, contractors, alumni, donors, vendors, visitors, or guests)? For questions or clarification, contact the Chief Compliance Officer at chansen@southalabama.edu, or 6-7115.	Yes No

Once submitted, the Dean/Department Head will receive an email indicating there is an agreement for review/approval. It is **imperative** that the reviewer ensure that the question regarding PHI is marked appropriately, so a Business Associate Agreement is not overlooked in the process of executing the contract(s). The University Legal team will ensure the BAA is executed when the Agreement Tracking System indicates PHI is involved.

USA HEALTH

Best Practices in Security

USA HEALTH

Password Control

Treat Your Password Like Your Toothbrush

Choose a Good One

Don’t Share It

Don’t Recycle an Old One

Replace it Every Few Months

USA HEALTH

Safe Computing and Email Use

- PHI on mobile devices
- Email encryption
- 3rd party software

USA HEALTH

Ransomware and Phishing

Phishing attacks and ransomware are serious problems that can steal or disable access to data.

Both ransomware and phishing attacks are increasingly common and are having devastating affects on businesses of all sizes.

The financial impact of cybercrime in general – and phishing and ransomware in particular – is hard to assess for a variety of reasons, but the FBI estimates that ransomware alone cost organizations $209 million in just the first three months of 2021.
Global cybercrime damages are predicted to exceed $8 billion in 2022.

USA HEALTH

Phishing Emails

Spear Phishing - A highly targeted form of phishing that hones in on a specific group of individuals or organizations.

Whaling - A form of phishing, targeted at administrative/executive level individuals.

Cloning - Whereby a legitimate email is duplicated, but the content is replaced with malicious links or attachments.

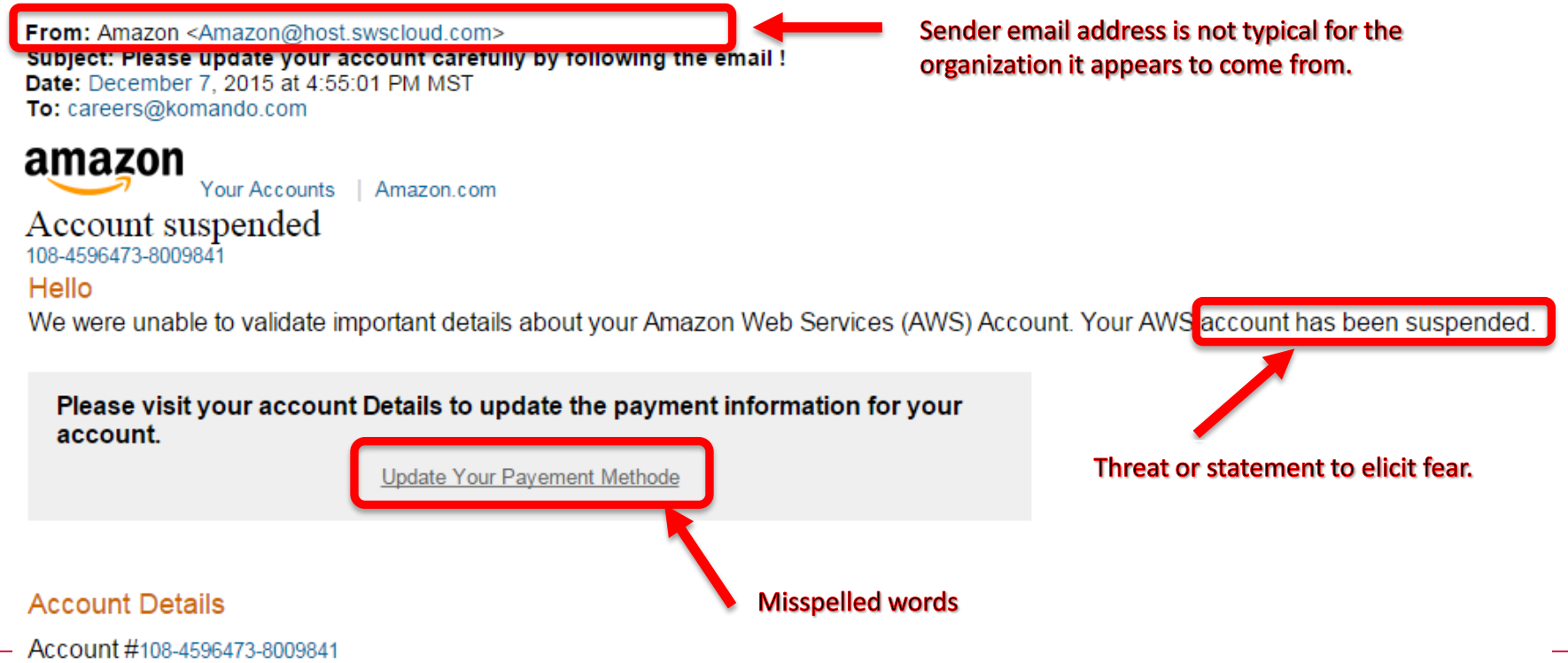
USA HEALTH

Anatomy of a Phishing Email

- **Contains Links or Attachments**
- **Poor Grammar and Spelling**
- **Requests Personal or Sensitive Information** (example: username and passwords)
- **High Sense of Urgency and/or Privacy**
- **Discusses Confidential Subjects** (example: salaries, security, etc.)
- **Incentivizes Through Threat or Reward**

USA HEALTH

Example



USA HEALTH

Ransomware

USA HEALTH

HIPAA Contacts

Linda Hudson – Chief Compliance Officer and HIPAA Privacy Officer
(251) 470-5802
lhudson@health.southalabama.edu

Carrie Pace –Senior Manager of IT Quality and Compliance and HIPAA Security Officer
(251) 471-7621
cpace@health.southalabama.edu