COOPERATIVE OF
AMERICAN PHYSICIANS

Essential Strategies

HIPAA 2.0

Welcome!

Scripps Mercy
PHYSICIAN
PARTNERS

What is HIPAA?

COOPERATIVE OF AMERICAN PHYSICIANS

Health Insurance Portability & Accountability Act., 1996

HIPAA regulations require all health care providers, organizations & business associates to develop / follow procedures that ensure the security & confidentiality of protected health information (**PHI, ePHI**) when being handled, received, transferred or shared (oral, paper or electronic).

HIPAA is enforced by the Office of Civil Rights (OCR).

HIPAA Compliancy

COOPERATIVE OF AMERICAN PHYSICIANS

- Notice of Privacy Practices **(NPP)**
- Patient Acknowledgements
- Protected Health Information **(PHI, ePHI)**
- Office Risk Assessment **(RA)**
- Business Associate Agreements **(BAA)**

COOPERATIVE OF
AMERICAN PHYSICIANS

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

Notice of Privacy Practices

(NPP)

Notice of Privacy Practices

COOPERATIVE OF AMERICAN PHYSICIANS

Requires that all covered health care providers develop and distribute a notice.

The notice must provide a clear, user-friendly explanation of individuals (patients) rights regarding **PHI, ePHI** & the privacy practices of the entity, health provider or health plan.

Notice of Privacy Practices

COOPERATIVE OF AMERICAN PHYSICIANS

NOTICE OF PRIVACY PRACTICES

[Physician Practice Name and Address]

[Name or Title and Telephone Number of Privacy Officer]

Effective Date:

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

We understand the importance of privacy and are committed to maintaining the confidentiality of your medical information. We make a record of the medical care we provide and may receive such records from others. We use these records to provide or enable other health care providers to provide quality medical care, to obtain payment for services provided to you as allowed by your health plan and to enable us to meet our professional and legal obligations to operate this medical practice properly. We are required by law to maintain the privacy of protected health information and to provide individuals with notice of our legal duties and privacy practices with respect to protected health information. This notice describes how we may use and disclose your medical information. It also describes your rights and our legal obligations with respect to your medical information. If you have any questions about this Notice, please contact our Privacy Officer listed above.

Must be posted or available!

Notice of Privacy Practices

COOPERATIVE OF AMERICAN PHYSICIANS

Why is This Important?

COOPERATIVE OF
AMERICAN PHYSICIANS

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

NPP - Patient Acknowledgements

NPP - Patient Acknowledgements

COOPERATIVE OF AMERICAN PHYSICIANS

Notice of Privacy Practices (HIPAA, PHI, ePHI, BAA):

- Accessible via poster or binder for patient and others
- Provide a fact sheet
- Signed receipt / acknowledgment form (physically or electronically)

NPP - Patient Acknowledgements

COOPERATIVE OF AMERICAN PHYSICIANS

[Physician Practice Name and Address]

[Name or Title and Telephone Number of Privacy Officer]

I hereby acknowledge that I received a copy of this medical practice's Notice of Privacy Practices. I further acknowledge that a copy of the current notice will be posted in the reception area, and that a copy of any amended Notice of Privacy Practices will be available at each appointment.

☐ I would like to receive a copy of any amended Notice of Privacy Practices by e-mail at: _____.

Signed: _____ Date: _____

Print Name: _____ Telephone: _____

If not signed by the patient, please indicate relationship:

☐ Parent or Guardian of minor patient

☐ Guardian or conservator of an incompetent patient

Name and Address of Patient: _____

Patient acknowledgement!

NPP - Patient Acknowledgements

COOPERATIVE OF AMERICAN PHYSICIANS

Why is This Important?

COOPERATIVE OF
AMERICAN PHYSICIANS

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

Business Associate Agreement

(BAA)

Business Associate Agreements

COOPERATIVE OF AMERICAN PHYSICIANS

Required with entities that:

- Create
- Receive e-health / diagnostic services
- Store / maintain any type of **PHI, ePHI**
- Transmit **ePHI** on behalf of a covered entity

Subcontractor:

- Subcontractor = person to whom a business associate delegates a function, activity, or service
- Subcontractor + **PHI** = Business Associate

Business Associate Agreements

COOPERATIVE OF AMERICAN PHYSICIANS

Business Associate Agreement

This Business Associate Agreement ("Agreement") is entered into this ___ day of _____-__, _____ between [covered entity], a California [professional corporation] [partnership] [sole proprietorship] ("Physician Practice ") and [business associate], a [state corporation] ("Contractor").

RECITALS

Physician Practice is a [type of organization] that provides medical services with a principal place of business at [address].

Contractor is a [type of organization] that [description of primary functions or activities] with a principal place of business at [address].

Physician Practice, as a Covered Entity under the Health Information Portability and Accountability Act of 1996 ("HIPAA") is required to enter into this Agreement to obtain satisfactory assurances that Contractor, a Business Associate under HIPAA, will appropriately safeguard all Protected Health Information ("PHI") as defined herein, disclosed, created or received by Contractor on behalf of, Physician Practice.

Physician Practice desires to engage Contractor to perform certain functions for, or on behalf of, Physician Practice involving the disclosure of PHI by Physician Practice to Contractor, or the creation or use of PHI by Contractor on behalf

Business Associate Agreements

COOPERATIVE OF AMERICAN PHYSICIANS

Why is This Important?

COOPERATIVE OF
AMERICAN PHYSICIANS

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

Breach Notifications

Breach Disclosure Duties

COOPERATIVE OF AMERICAN PHYSICIANS

Breach (45 C.F.R. § 164.406 - 164.410) :

Unauthorized acquisition, access, use, disclosure of unsecured **PHI, ePHI** in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of **PHI, ePHI.**

Covered entities and business associates are required to report any breach of unsecured **PHI, ePHI.**

Breach Disclosure Duties

COOPERATIVE OF AMERICAN PHYSICIANS

Less than 500 patients:

Covered entities and business associates are required to notify OCR of breach *no later than* 60 days of calendar year end.

- Notify your Medical Professional Liability Carrier

- Follow breach instructions:

www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Breach Disclosure Duties

COOPERATIVE OF AMERICAN PHYSICIANS

Greater than 500 patients:

Required to notify OCR *within* 60 days of breach.

- Must notify the media
- Offer affected patients 1 year credit monitoring service
- Notify your Medical Professional Liability Carrier

- Follow breach instructions:

www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Breach Disclosure Duties

COOPERATIVE OF AMERICAN PHYSICIANS

Why is This Important?

COOPERATIVE OF
AMERICAN PHYSICIANS

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

Office Risk Assessment

(RA)

Office Risk Assessment

COOPERATIVE OF AMERICAN PHYSICIANS

- A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards.
- Risk assessments may reveal areas where your organization's protected health information (**PHI, ePHI**) may be at risk.

Risk Assessment

COOPERATIVE OF AMERICAN PHYSICIANS

HIPAA Sections	HIPAA Security Rule Standard Implementation Specification	Implementation	Requirement Description	Solution	Yes/No/Comments
164.308(a)(1)(i)	*Security Management Process*	Required	Policies and procedures to manage security violations		
164.308(a)(1)(ii)(A)	Risk Analysis	Required	Conduct vulnerability assessment	Penetration t[est], vulne[rability] assessment	
164.308(a)(1)(ii)(B)	Risk Management	Required	Implement security measures to reduce risk of security breaches	Sil[ent] [patch] management, vu[lnerability] [manage]ment, asset ma[nage]ment, helpdesk	
164.308(a)(1)(ii)(C)	Sanction Policy	Required	Worker sanction for policies and procedures violations	[Sec]urity policy document [man]agement	
164.308(a)(1)(ii)(D)	Information System Activity Review	Required	Procedures to [review] activity	Log aggregation, log ana[lysis], security event management, host IDS	
164.308(a)(2)	*Assigned Security Responsibility*	Required	Ide[ntify] [who] responsible for policies and procedures		
164.308(a)(3)(i)	*Workforce Security*	Required	Implement policies and procedures to ensure appropriate PHI access		
164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Addressable	Authorization/supervision for PHI access	[Mandatory, discretionary and role-based] access control: ACL, native OS policy enforcement	
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Addressable	Procedures to ensure appropriate PHI access	Background checks	
164.308(a)(3)(ii)(C)	Termination Procedures	Addressable	Procedures for terminating PHI access [security policy enforcement management]	Single sign-on, identity management, access controls	
164.308(a)(4)(i)	*Information Access Management*	Required	Policies and procedures to authorize access to PHI		
164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	Required	Policies and procedures to separate PHI from other operations	Application proxy, firewall, mandatory VPN, SOCKS	
164.308(a)(4)(ii)(B)	Access Authorization	Addressable	Policies and procedures to authorize access to PHI	Mandatory, discretionary and role-based access control	
164.308(a)(4)(ii)(C)	Access Establishment and Modification	Addressable	Policies and procedures to grant access to PHI	Security policy document management	
164.308(a)(5)(i)	*Security Awareness Training*	Required	Training program for workers and managers		
164.308(a)(5)(ii)(A)	Security Reminders	Addressable	Distribute periodic security updates	Sign-on screen, screen savers, monthly memos, e-mail, banners	

Assessment Checklist

Risk Assessment

COOPERATIVE OF AMERICAN PHYSICIANS

Risk No	Vulnerability	Threat	Risk	Risk Summary	Likelihood	Impact	Overall Risk	Recommendations
1	Password changes are not enforced and set to no-expire	Malicious Use	Confidentiality of org. data	Compromise of password could results in data breach and/or loss of org.	Medium	High	Medium	The IT Operations teams should enable the functionality within Active Directory or database to reset password every 15 days. Password policies are to be documented in IT Controls document
2								
3								
4								

Risk Assessment

COOPERATIVE OF AMERICAN PHYSICIANS

Why is This Important?