COOPERATIVE OF
AMERICAN PHYSICIANS

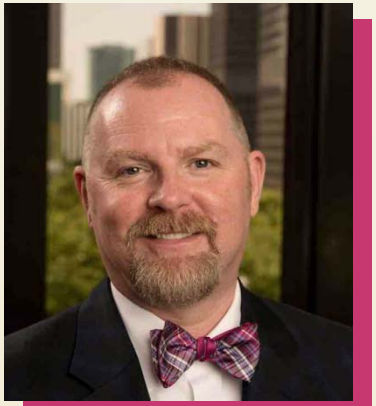
ESSENTIAL STRATEGIES

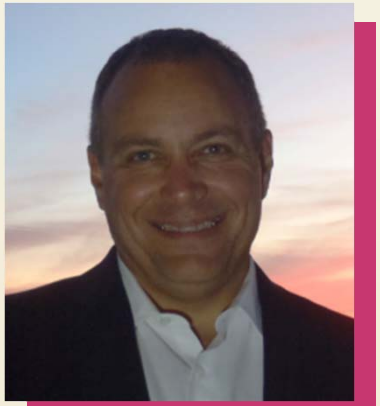
HIPAA 2.0

Welcome!

Essential Strategies

HIPAA 2.0





Allan Ridings

Senior Risk Management & Patient Safety Specialist – Cooperative of American Physicians, Inc.

- **30 years of practice management experience**
- **Nationally published on HIPAA and eHealth**

Jeff Mongelli

CEO, Acentec, Inc.

- **15 years of health care IT experience**
- **Nationally published on health care IT security**

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec

Improving Medical Practice Performance®

Essential Strategies

OBJECTIVES:

- Identify components of HIPAA compliancy
- Describe recent changes in HIPAA
- Sharing protected health information
- Restricting protected health information

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec

Improving Medical Practice Performance®

Essential Strategies

HEALTH INFORMATION PRIVACY

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Overview:

Health Insurance Portability & Accountability Act of 1996 (**HIPAA**)

What is HIPAA?

HIPAA regulations require all health care providers, organizations, and business associates to develop / follow procedures that ensure the security and 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 Benefits

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

- Supporting obligations
- Supporting compliance
- Secured records
- Knowledgeable staff
- Reduced risk

HIPAA Compliancy

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

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

HIPAA Compliancy

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

- E-mailing of **ePHI**
- Copying / Releasing **PHI**
- Childhood / Student Immunizations

HIPAA Compliancy

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

- Disclosure Duties
- Unapproved Access to **PHI, ePHI** (breach)
- Sale of **PHI**

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Notice of Privacy Practices

(NPP)

Notice of Privacy Practices

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**, and the privacy practices of the entity, health provider, or health plan.

NPP - Patient Acknowledgements

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

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)

Notice of Privacy Practices

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

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.

NPP - Patient Acknowledgements

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

[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!

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

COOPERATIVE OF
AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Releasing Protected Health Information (**PHI, ePHI**)

PHI - Release Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Affected individuals must be notified:

- When types of uses and disclosures require authorization
- That disclosures will be made only with authorization
- If any information is used for marketing or sold

An individual may revoke authorization.

PHI - Release Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Why this matters:

- The Office for Civil Rights has stated the next big HIPAA update will be regarding ACCOUNTING FOR DISCLOSURES (it's past due).

PHI - Release Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Written authorizations:

- Are required for inspection and/or release of billing notes or any part of a medical record.
- A separate authorization is required for each release. *(with exceptions)*

PHI - Release Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Time:

- Inspection of records honored within 5 working days
- Copies must be released within 15 calendar days
- Have uniformed policy, educated staff

PHI - Release Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Applicable Charges:

- Reasonable clerical fees, plus 25¢ per page
- $15 maximum clerical fee for subpoena copy services
- Records to support an appeal for a public benefit program provided at no charge and within 30 days
- When released on CD or USB thumb-drive, you may charge for the labor and media

PHI - Release Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Applicable Exceptions:

Health care providers and other entities that participate in an Organized Health Care Arrangement (**OHCA**)

All entities, sites, and locations may share medical information with each other for treatment, payment, and health care operations purposes. [45 CFR 164.520(d)]

PHI - Release Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

HIPAA Privacy during emergencies (11/2014):

- Treatment during emergencies
  [45 CFR 164.502(a)(1)(ii), 164.506(c), 164.510(b)]
- Public Health Activities - CDC & Public Heath Authorities
- Imminent threat to public health
  [45 CFR 164.512(b)(1)(i)]

PHI - Release Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Physician Notification & Review:

- Review all requests that arrive to your offices

Documentation:

- Who, Where, When (disclosure log)

PHI - Personal Request Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

AUTHORIZATION FOR USE AND DISCLOSURE OF MEDICAL INFORMATION

This authorization allows the healthcare provider(s) named below to release confidential medical information and records. Note: *Information and records regarding treatment of minors, HIV, psychiatric/mental health conditions, or alcohol/substance abuse have special rules that require specific authorization.*

AUTHORIZATION

I hereby authorize: _____
Physician/Healthcare Facility

To release information regarding my medical history, illness or injury, consultation, prescriptions, treatments, diagnosis or prognosis, including x-rays, correspondence and/or medical records (including those from my other health care providers that the above named health care provider may hold), by means of mail, fax, or other electronic methods.

To: _____
Name

_____
Address

_____ _____ _____
City State Zip Code

The medical information/records will be used for the following purpose: _____

Personal

This authorization is:
[ ] Unlimited (all records, excluding Substance Abuse, Mental Health, HIV Diagnosis/Treatment)
[ ] Limited to the following medical information: _____

I also consent to the specific release of the following records:

Drug/Alcohol/Substance Abuse_____(initial) HIV Diagnosis/Treatment _____(initial)
Psychiatric/Mental Health _____(initial) Genetic Information _____(initial)
Tests for Antibodies to HIV _____(initial)

DURATION This authorization shall be effective immediately and remain in effect until _____
Date

Future Date

RESTRICTIONS

PHI - Release To / From Authorization

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

AUTHORIZATION FOR USE AND DISCLOSURE OF MEDICAL INFORMATION

This authorization allows the healthcare provider(s) named below to release confidential medical information and records. Note: *Information and records regarding treatment of minors, HIV, psychiatric/mental health conditions, or alcohol/substance abuse have special rules that require specific authorization.*

AUTHORIZATION

I hereby authorize: _____
Physician/Healthcare Facility

To release information regarding my medical history, illness or injury, consultation, prescriptions, treatments, diagnosis or prognosis, including x-rays, correspondence and/or medical records (including those from my other health care providers that the above named health care provider may hold), by means of mail, fax, or other electronic methods.

To: _____
Name

_____
Address

_____ _____ _____
City State Zip Code

The medical information/records will be used for the following purpose: _____

Continuity

This authorization is:
[ ] Unlimited (all records, excluding Substance Abuse, Mental Health, HIV Diagnosis/Treatment)
[ ] Limited to the following medical information: _____

I also consent to the specific release of the following records:

Drug/Alcohol/Substance Abuse_____(initial) HIV Diagnosis/Treatment _____(initial)
Psychiatric/Mental Health _____(initial) Genetic Information _____(initial)
Tests for Antibodies to HIV _____(initial)

DURATION This authorization shall be effective immediately and remain in effect until_____
Date

Specific Date

RESTRICTIONS

Childhood Immunization Records

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

A Covered Entity *may* release student or childhood immunization records to a school/college without authorization:

- If state law requires a school to have an immunization record on file

- Written or oral agreement (must be documented)

PHI - Disclosure Log

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

DISCLOSURE LOG

PATIENT NAME:_____
LAST FIRST MI MAIDEN OR OTHER NAME

DATE OF BIRTH:___-___-___ MEDICAL RECORD #:_____
MO DAY YR

ADDRESS:_____ _____CITY:_____STATE:____ZIP:_____

DAY PHONE:_____ _____ EVENING PHONE:_____

Use this log to record any disclosure of the patient's protected health information that is not for treatment, payment, or health care operations, or pursuant to the patient's Authorization

Date of Disclosure	Name and Address to whom disclosed	Description of information disclosed	Purpose of disclosure

Essential Strategies:

HIPAA COMPLIANCY

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

E-mailing & Texting Patients

E-mail & Texting ePHI

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Code of Federal Regulations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

What is needed...
when we e-mail
or text patients?

Code of Federal Regulations

CFR requires encryption when e-mailing or texting electronic protected health information (ePHI).

Code of Federal Regulations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

A covered entity must:

- Implement a mechanism to encrypt and decrypt electronically protected health information (45 CFR § 164.312)

- Be in accordance with privacy rule (45 CFR § 164.306)

Code of Federal Regulations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Access rights require a covered entity to:

- Use Advanced Encryption Standard (AES) encryption, either 128-bit or 256-bit
- Implement technical policies and procedures for systems that maintain electronic protected health information 164.308(a)(4) [Information Access Management]

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Treatment, Payment
& Operations
(TPO)

Treatment, Payment, Operations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Treatment:

- Medical care, all in-office, e-health, m-health, t-health

Payment:

- Referrals
- Medical billing office, claims, internal /external services

Operations:

- Medical office policies /procedures
- Office rules and regulations /business policies

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

COOPERATIVE OF

AMERICAN PHYSICIANS

Acentec

Improving Medical Practice Performance®

Business Associate Agreement

(BAA)

Business Associate Agreements

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

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:

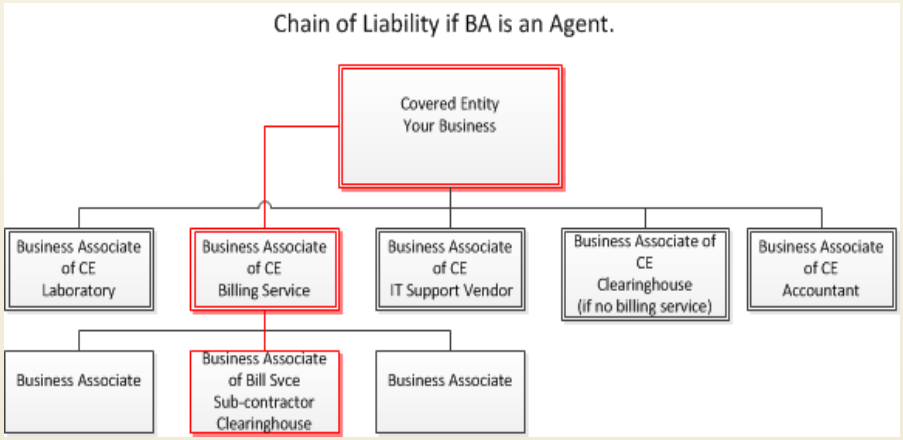
- Subcontractor = person to whom a business associate delegates a function, activity, or service
- Subcontractor + **PHI** = Business Associate

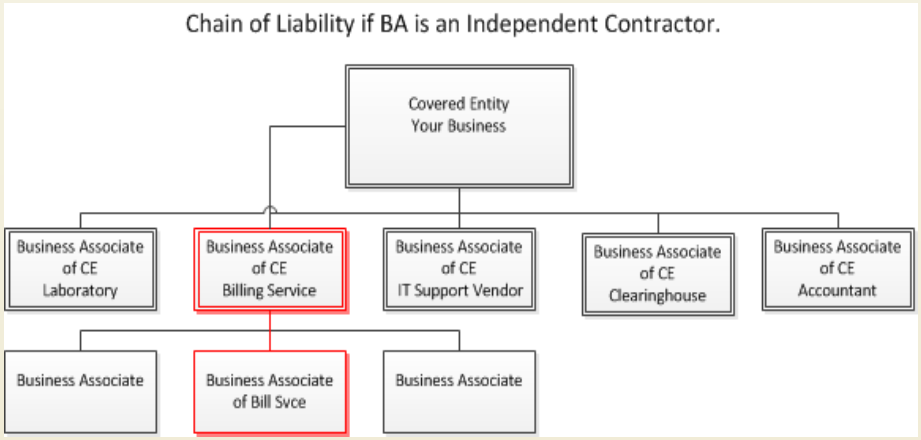
Business Associate Agreements

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Agency vs. Independent Contractor





Business Associate Agreements

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

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

Acentec
Improving Medical Practice Performance®

Is this person a Business Associate?

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Breach Notifications

Breach Disclosure Duties

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

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

Acentec
Improving Medical Practice Performance®

Do we HAVE to notify patients?:

"… breach notification is necessary in all situations except those in which the CE demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment …"

Section 160.402

Breach Disclosure Duties

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

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

Acentec
Improving Medical Practice Performance®

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

Acentec
Improving Medical Practice Performance®

***Incident Risk Assessment (IRA)*:**

An Incident Risk Assessment should include:

- the nature and extent of the PHI involved;
- the unauthorized person who used the PHI or to whom the PHI was disclosed;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk to the PHI has been mitigated.

The IRA is only required if the CE, based on the facts, wants to demonstrate that no notification is required.

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

COOPERATIVE OF
AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Office Risk Assessment

(RA)

Office Risk Assessment

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

- 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

Acentec
Improving Medical Practice Performance®

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[illegible] vulnerability assessment	
164.308(a)(1)(ii)(B)	Risk Management	Required	Implement security measures to reduce risk of security breaches	S[illegible] patch management, vu[illegible] management, asset ma[illegible]ment, helpdesk	
164.308(a)(1)(ii)(C)	Sanction Policy	Required	Worker sanction for policies and procedures violations	[illegible]urity policy document management	
164.308(a)(1)(ii)(D)	Information System Activity Review	Required	Procedures to [illegible] system activity	Log aggregation, log anal[illegible] security event management, host IDS	
164.308(a)(2)	*Assigned Security Responsibility*	Required	Ide[illegible] of 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 S[illegible]	Addressable	Authorization/supervision for PHI acc[illegible]	[illegible]datory, discretionary and role-based access control: ACL, native OS policy enforcement	
164.308(a)(3)(ii)(B)	Workforc[illegible]e Procedur[illegible]	Addressable	Procedures to ensure appropriate PHI access	Background checks	
164.308(a)(3)(ii)(C)	Terminatio[illegible]ocedures	Addressable	Pro[illegible]es for terminating PHI access [illegible]ment management	Single sign-on, identity management, access controls	
164.308(a)(4)(i)	*Information Access Management*	Required	[illegible]cies and procedures to authorize [illegible]s to PHI		
164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	[illegible]	Policies and procedures to separate PHI from other operations	Application proxy, firewall, mandatory UPN, 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

Acentec
Improving Medical Practice Performance®

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								

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Let's review what's required of you…

Medical Office Requirements #1

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Secure registration process:

- Face-to-face
- Patient portal (**EHR**)

Notice of Privacy Practices - HIPAA / PHI, ePHI:

- Poster, notice, or binder
- Signature acceptance

Business Associate Agreements (BAA)

- Transmit **ePHI** on behalf of a covered entity

Medical Office Requirements #2

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

HIPAA education training for all staff:

- Sign-in sheet
- Signature understanding / acceptance

Risk Assessment:

- Regularly scheduled assessments

8 Most Common Causes of Violations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

#1 Authorized Users

- Users that have legitimate access to sensitive information are the weakest link in information security
- Sharing passwords
- Exposing passwords (taped to monitor)
- Giving out passwords
- Sending PHI to incorrect destinations
- Sharing PHI on social media
- Discussing PHI with others or in front of others

8 Most Common Causes of Violations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

#2 Failure to Conduct or Update Risk Assessment

- BCBS Tennessee ($1.5 M)
  - Failure to re-evaluate threats/vulnerabilities to ePHI caused by changing operational environment and manage risk
- Alaska DHSS ($1.7M)
  - Failure to conduct a risk analysis to identify location and safeguards for PHI, training, and controls for portal devices
- Mass. St. Elizabeth's Medical Center (SEMC) ($218,000)
  - Has agreed to settle potential violations of HIPAA … for use of an Internet-based document sharing product and failure to timely notify OCR

8 Most Common Causes of Violations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

#3 Failure to Consider or Properly Implement New Technology

- E-mail encryption
- Backup encryption
  - Massachusetts Eye and Ear Institute ($1.5M)
  - Stolen personal laptop of physician using device as desktop substitute
  - Covered entity had not implemented a program to mitigate identified risks to ePHI
  - Encrypt data stored on end-user devices

8 Most Common Causes of Violations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

#4 Failure to Identify Business Associates

- Phoenix Cardiac Surgery ($100K)
- Backup encryption
  - ePHI disclosed through Internet when provider used third party application hosted in the cloud

Business associate agreements are required when sharing data with cloud computing service providers!

8 Most Common Causes of Violations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

#5 Failure to Create Culture of Compliance Among Workforce

- Culture of Convenience remains the prevailing practice in medicine
- CSMC – settled violations related to disclosure of PHI of celebrity patients for $865,500
- Sharing of passwords, etc.
- No enforcement of policies, i.e., “everyone is doing it”

8 Most Common Causes of Violations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

#6 Failure to Remember Patient Rights

- Cignet Health fined $4.3 million for refusing to provide access to medical records upon patient's request. ($3 million attributed to "willful neglect" for refusing to comply with investigative requests.)
- Right to amend information.
- OCR examples
  - Failure to allow access to whole record (because part of it was created by another provider).

8 Most Common Causes of Violations

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

#6 Failure to Remember Patient Rights (cont.)

- Attempt to condition privacy rule compliance on patient's agreement to not disclose information about physician (we won't tell if you don't tell) (Yelp)

- Failure to accommodate a reasonable request for confidential communications (patient requested to be contacted only on mobile phone, not at home – but the treatment reminder was left on home voicemail)

8 Most Common Causes of Violations

COOPERATIVE OF AMERICAN PHYSICIANS

#7 Forgetting About "Reasonable Safeguards"

- Discussion of PHI in front of other patients, in waiting rooms
- Paper PHI not safeguarded from theft
- Information faxed to patient's employer did not include confidentiality statement on cover sheet
- Massachusetts General Hospital – Paid $1,000,000 to settle violations related to loss of PHI of 192 patients on subway train from infectious disease outpatient practice (including HIV/AIDS patients)

8 Most Common Causes of Violations

COOPERATIVE OF AMERICAN PHYSICIANS

#8 Forgetting the Minimum Necessary Rule

- Failure to distribute information on a “need to know” basis
  - Example: OR schedule sent to people who had no need for the information – complainant was an employee/patient
- Computer access and paper access

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

Questions…

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

Essential Strategies:

HIPAA COMPLIANCY

The information in this presentation should not be considered legal advice applicable to a specific situation.

Legal guidance for individual matters should be obtained from a retained attorney.

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec

Improving Medical Practice Performance®

ESSENTIAL STRATEGIES:

HIPAA COMPLIANCY

Allan Ridings
Cooperative of American Physicians, Inc.
Phone: 800-252-7706
Email: riskmanagement@CAPphysicians.com
Web: www.CAPphysicians.com

Jeff Mongelli, CEO
Acentec, Inc.
Phone: 949-474-7774
Email: jeffm@acentec.com
Web: www.acentec.com

COOPERATIVE OF AMERICAN PHYSICIANS

Acentec
Improving Medical Practice Performance®

COOPERATIVE OF
AMERICAN PHYSICIANS

Thank You!