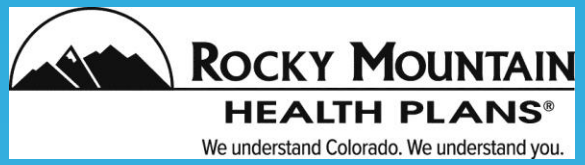
HIPAA Security and Privacy Training for Rocky Mountain Health Plans' Vendors and Business Associates



Disclaimer:

The following presentation is for informational/educational purposes only. It is not tailored to any specific situation.

Nothing contained in this presentation constitutes legal advice.

This information is based on current federal regulations and subject to change based on changes in federal law or subsequent interpretive guidance.

You need to check your state's law regarding the issues in this presentation as some state's laws may be more stringent than federal law in some cases or state law exceptions may apply.

You should evaluate all information provided in this presentation in consultation with your legal or other adviser, as appropriate.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

Rocky Mountain Health Plans ("RMHP") is committed to complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), all subsequent amendments, and any associated laws and regulations.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

RMHP expects our Business Associates and other vendors to:

1) be aware of their obligations under HIPAA, and
2) be committed and able to comply with the requirements as well.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA OVERVIEW

HIPAA: Health Insurance Portability and Accountability Act

- Originally enacted in 1996
- A federal law that in part ensures an individual's health information is protected (PHI)
- Many parts: TCS, NPI, HPID, SECURITY, BREACH NOTICE, PRIVACY
- Contains provisions for enforcement and PENALTIES for violations
- Amended over the years, most recently by the Health Information Technology for Economic and Clinical Health Act (HITECH)
- Applies to Covered Entities (CE):

  Healthcare Providers, Health Plans, Health Care Clearinghouses

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HITECH ACT

- ✓ Expanded application of some HIPAA Privacy and Security Rules to Business Associates (BA) – *prior liability based only on contractual obligations with CE*
- ✓ BA definition expanded (inclusion of subcontractors)
- ✓ New breach notification rules for CEs and for BAs
- ✓ Limited certain uses/disclosures of PHI
- ✓ Significant increase in potential penalties!!!!

  BAs can be directly liable for penalties

Business Associates are persons/entities, outside of CE's workforce, who create, maintain, receive, or transmit PHI for some function or activity on behalf of the CE. Some common examples: claims processing, legal, accounting, quality improvement, billing, etc...

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

SANCTIONS FOR VIOLATIONS OF HIPAA

- ✓ CE can be held liable for employee or BA violations through Federal common law agency principles
- ✓ BA can be held liable for employee or subcontractor violations (same basis)
- ✓ Civil Monetary Penalties (CMPs):

  Amount depends of several factors: level of culpability; # of people affected; amount and type of harm inflicted; entities history, etc…
- ✓ Possible Criminal Prosecution
- ✓ Civil Actions by State Attorney Generals on behalf of their state's citizens under HITECH Act.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

KEY HIPAA DEFINITION: PROTECTED HEALTH INFORMATION

Protected Health Information (PHI) is:

Any information collected from an individual, including demographic information, that:

- Relates to the physical or mental health of an individual
- The treatment of those conditions
- The provision of health care
- The payment for health care
- Identifies, or provides a basis to identify, an individual

PHI can be in any form: verbal, written, or electronic

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA SECURITY RULE

Subpart C – Security Standards for the Protection of Electronic Protected Health Information; 45 CFR 164.302 – 164.318

Focus is on the *availability*, *confidentiality*, and *integrity* of electronic PHI.

Availability means that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means that data or information is not made available or disclosed to unauthorized persons or processes.

Integrity means that data or information has not been altered or destroyed in an unauthorized manner.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

THE SECURITY RULE PARTS

- ✓Security standards; General rules
- ✓Administrative Safeguards
- ✓Physical Safeguards
- ✓Technical Safeguards
- ✓Organizational Requirements
- ✓P&Ps and documentation requirements

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA SECURITY RULES REQUIRE...

Administrative, *Technical*, and *Physical* safeguards be in place to protect privacy of E-PHI.

Administrative safeguards are actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

SECURITY STANDARDS – GENERAL RULES

RMHP as a Covered Entity (and our BAs) must

1) ensure the confidentiality, integrity, and availability of all E-PHI we create, receive, maintain or transmit.

2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted under the Privacy Rule.

4) ensure compliance by the workforce.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

ADMINISTRATIVE SAFEGUARDS

Standard: Security Management Process

CEs must "implement policy and procedures to prevent, detect, contain, and correct security violations.

> Implementation Specifications: Risk Analysis, Risk Management, Sanction Policy, Info. System Activity Review

Risk analysis and risk management are the basis for all security activities. CE's must understand what threats they face, and the risk they are exposed to. It is only then that a plan can be developed to address or manage those vulnerabilities.

CE's also need to have appropriate sanctions in place so their workforce is encouraged to comply with the security management plan.

CE's should also regularly review their Information Systems (i.e. audit logs, access reports, etc…) to monitor compliance.

ADMINISTRATIVE SAFEGUARDS

Standard: Assigned Security Responsibility

CE's must "identify the security official who is responsible for the development and implementation of the policies and procedures required" under the security rule.

Standard: Security Incident Procedure

CE's must "implement policies and procedures to address security incidents."

Implementation Specification: Response Reporting

Security incidents should be identified, responded to, mitigated to the extent possible, and then documented completely.

What happens if:

Someone loses a laptop?

Someone breaks into your facility?

> ***Security incident*** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

ROCKY MOUNTAIN HEALTH PLANS®

We understand Colorado. We understand you.

ADMINISTRATIVE SAFEGUARDS

Standard: Workforce Security

CE's must "implement policies and procedures to ensure that all members of its workforce have appropriate access" to ePHI including preventing any workforce members that should not have access to ePHI from having access.

Implementation Specifications: Authorization and/or Supervision, Workforce Clearance Procedure, Termination Procedure.

CE's must ensure policies regarding access to PHI a workforce member is given is appropriate to their job duties. If they do not need access to perform their job, they should not have access.

CE's also must have procedures for terminating access once a workforce member no longer requires access (i.e. terminated, change of positions).

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

ADMINISTRATIVE SAFEGUARDS

Standard: Information Access Management

CE's must "implement policies and procedures for authorizing access to ePHI that are consistent" with the security rule.

Implementation Specifications: Access Authorization, Access Establishment and Modification

The previous standard "Workforce Security" dealt with the policies and procedures addressing the whole workforce, this standard addresses how you actually implement the authorization/access.

The process for allowing access could involve the documented steps needed for access (i.e. getting passwords, supervisor approval, etc…). Policies and procedures should also address how changes to a workforce member's authorization is accomplished.

ADMINISTRATIVE SAFEGUARDS

Standard: Security Awareness and Training

CE's must "implement a security awareness and training program for all members of its workforce (including management).

Implementation Specifications: Security Reminders , Malicious Software Protection, Log-in Monitoring, Password Management

Security training is required of **all** workforce members. Consistent security reminders reinforce the importance of compliance. No specific method is required, but any reminders implemented need to be documented.

Workforce members should be reminded of the security measures designed to protect Information Systems. Policies and procedures should address malicious software downloads, log-in monitoring, and password management.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

ADMINISTRATIVE SAFEGUARDS

Standard: Contingency Plan

CE's must "establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence… that damages systems that contain ePHI."

> Implementation Specifications: Data Backup Plan, Disaster Recovery Plan, Emergency Mode Operation Plan, Testing and Revision Procedure, Application and Data Criticality Analysis

Being able to recover from a natural disaster, an act of vandalism, employee malfeasance, or other emergency depends on being able to reproduce or recover the information on the damaged information systems. Arrangements also need to be made for how the organization will operate while recovering from any interruptions . Finally, evaluate systems and applications to determined their priority for restoration.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

ADMINISTRATIVE SAFEGUARDS

Standard: Evaluation

CEs must "perform periodic technical and nontechnical evaluation" of all standards, modify accordingly & analyze policies and procedures and operations.

Standard: Business Associate Agreements

CEs "may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entities behalf only" if the CE receives satisfactory assurances the ePHI will be appropriately safeguarded.

Implementation Specification: Written Contracts

Written contracts must detail the parameters of the agreement.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

PHYSICAL SAFEGUARDS

Standard: Facility Access Controls

CEs must "implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed while assuring that properly authorized access is allowed."

> Implementation Specifications: Contingency Operations, Facility Security Plan, Access Control and Validation Procedure, Maintenance Records

Plans need to be in place to address how the appropriate persons have access to systems in a disaster or emergency situation. During normal operations, plans should address safeguarding the facility and equipment, controlling and validating who has access, and keep accurate and complete records of any repairs or modifications to the facility.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

PHYSICAL SAFEGUARDS

Standard: Workstation Use

CEs must implement policies and procedures that specify the proper functions to be performed, and the physical attributes of the surroundings of a specific workstation that can access ePHI.

Standard: Workstation Security

CEs must implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

PHYSICAL SAFEGUARDS

Standard: Device and Media Controls

CEs must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility.

> Implementation Specifications: Disposal, Media Re-use, Accountability, Data Backup and Storage

Electronic storage media must be disposed of securely. Devices should also never be reused before all of the information on the device is removed. Any devices that contain ePHI must be accounted for, and who is responsible for those devices should be clear. Finally, if a storage device is to be serviced or moved, any ePHI on that device should be backed up in case of an accidental loss.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

TECHNICAL SAFEGUARDS

Standard: Access Control

CEs must implement technical polices and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

> Implementation Specifications: Unique User IDs, Emergency Access Procedures, Automatic Logoff, Encryption & Decryption

Every user of the system must have an unique identifier so that CEs can monitor who had access to and what they did in the system. Procedures also must be in place that would allow users to access ePHI during an emergency.

Automatic logoff is an effective method of preventing unauthorized access. Additionally, encryption of the ePHI protects it from being accessed or viewed by unauthorized persons.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

TECHNICAL SAFEGUARDS

Standard: Audit Control

CEs must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Standard: Integrity

CEs must implement policies and procedures to protect ePHI from improper alteration or destruction.

Implementation Specification: Mechanism to authenticate ePHI

There must be controls in place to maintain the integrity of ePHI on the information system.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

TECHNICAL SAFEGUARDS

Standard: Person or Entity Authentication

CEs must implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

Standard: Transmission Security

CEs must implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communication network.

Implementation Specifications: Integrity Controls, Encryption

Focus is on the integrity of the information while being transmitted to ensure the data sent is the same data received. Encryption seeks to assure that only the intended recipient will be able to access the data.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

POLICY & PROCEDURES AND DOCUMENTATION

- ✓ Must implement reasonable and appropriate P&Ps
- ✓ Must maintain written or electronic documentation of P&Ps (and any assessment) for 6 years from date of creation or when last in effect, whichever is later
- ✓ P&Ps must be available and reviewed and updated as necessary.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

SUBPART E – PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION; 45 CFR 164.500 – 164.534

Uses and Disclosures of PHI; General Rules (164.502)

Uses and Disclosures; Organizational requirements (164.504)

Uses and Disclosures for TPO (164.506)

Uses and Disclosures needing authorization (164.508)

Uses and Disclosures requiring opportunity to agree or object (164.510)

Uses and Disclosures not requiring authorization or opportunity to object (164.512)

Other requirements relating to uses and disclosures of PHI (164.514)

Notice of Privacy Practices (164.520)

Right to request privacy protection of PHI (164.522)

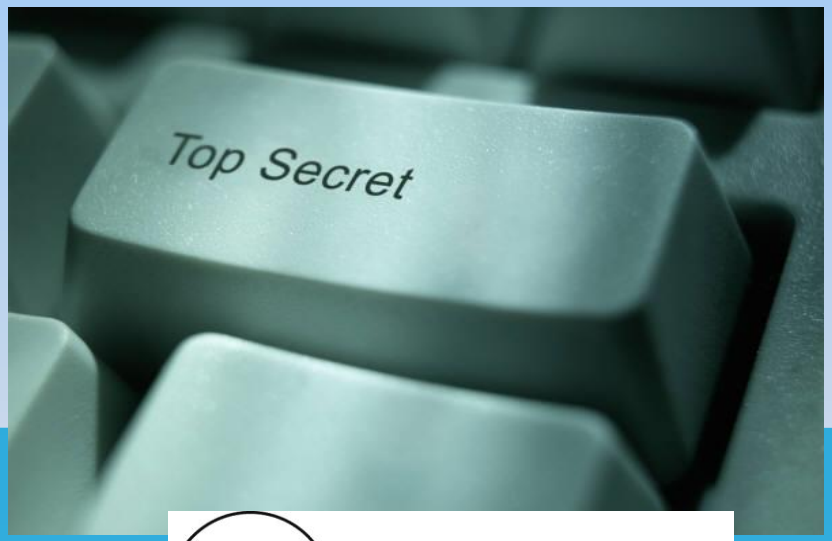
Access of Individuals to PHI (164.524)

Amendment of PHI (164.526)

Accounting for disclosures of PHI (164.528)

Administrative requirements (164.530)

Transition provisions (164.532)



ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY – GENERAL RULES

Permitted Uses and Disclosures:

- To the individual
- For Treatment, Payment, or Health Care Operations (TPO)
- Incident to authorized use / disclosure

Required Disclosures:

- To the individual (with certain exceptions)
- To Department of Health & Human Services (DHHS) as part of compliance investigation of CE

BA permitted to use/disclose PHI according to BA Agreement or as required by law

BA must disclose to DHHS as part of compliance investigation

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY – GENERAL RULES

Prohibited Uses and Disclosures:

- Genetic Information for underwriting purposes
- Sale of PHI

Minimum Necessary:

- When using or disclosing PHI reasonable efforts must be made to limit the amount to the minimum necessary to accomplish intended purpose.
- Does not apply to uses or disclosure:
  - for treatment by health care provider
  - to the individual
  - required by law or to DHHS in compliance investigation

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY – GENERAL RULES

Deceased Individuals:

PHI protected for 50 years following the death of an individual

Personal Representatives (PR):

If truly a PR, treat as the individual

Adults & Emancipated Minors: must have documentation proving the authority to act for individual under applicable law (i.e. power of attorney, executor of estate)

Unemancipated Minors:

parents, guardians, etc… stand in place of minor UNLESS minor has authority to act on own, or consented to treatment, or can consent. However, check State law for granting or prohibition of access.

HIPAA PRIVACY – GENERAL RULES

Business Associate Contracts:

- must establish the permitted and required uses and disclosures
- may permit use/disclosure for proper management and administration of CE
- may provide data aggregation related to healthcare operations of CE
- must contain certain required elements
- must authorize termination of contract by CE if BA violates material terms

BAs may contract with sub-contractors – another BA:

- same restrictions must be included in agreements

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY – TPO

Can use or disclose PHI

To providers for treatment

To other health plans, providers, billing company/clearinghouse for:

payment activity, or

health care operations activity

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: AUTHORIZATIONS

- Written Authorizations
  - Except for TPO, or required disclosures, must have authorization to disclose PHI outside the company
  - Internal use or disclosure of PHI:
    - For Marketing communications
    - For Research activities
    - Involving psychotherapy notes
  - Specific elements must be in an authorization

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: AUTHORIZATIONS (CONT.)

Written Authorizations

- Disclosure must be consistent with terms of authorization
- Psychotherapy Notes – need authorization except for
  - TPO or Required Disclosures
- Marketing Uses need authorizations, limited exceptions
- Sale of PHI need authorization and info re: remuneration

Must be in plain language.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: OPPORTUNITY TO AGREE / OBJECT

May get oral permission to disclose

To family, friends, etc… information relevant to the family's or friend's involvement in individual's care or payment for care

If individual is present, and has competency to make healthcare decisions, individual can give verbal consent

Consent can be inferred based on professional judgment

If individual not present, incapacitated, or in emergency:

can disclose information relevant to person's involvement to individual's care if in individual's best interest in CE's professional judgment

Deceased individuals' PHI can be disclosed to family, friends if PHI is relevant to family's, friend's involvement in Individual's care before they died

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: NO AUTHORIZATION OR OPPORTUNITY TO AGREE/OBJECT REQUIRED

When required by law

For public heath activities

About victims of abuse, neglect, or domestic violence

For health oversight activities

For judicial or administrative proceedings or law enforcement purposes

About decedents

For cadaveric organ, eye or tissue donation purposes

For limited research purposes

To avert a serious threat to health and safety (good faith requirement)

For specialized government functions

For worker's compensation purposes

ROCKY MOUNTAIN HEALTH PLANS®

We understand Colorado. We understand you.

HIPAA PRIVACY: OTHER REQUIREMENTS RELATED TO USE AND DISCLOSURE

De-identified Information is not PHI!

Can de-identify PHI by removal of:

Names	Geographic info	Dates (i.e DOB)
Telephone #s	Fax #s	Email addresses
SSN	Medical record #	Health Plan #
Account #	Certificate/License #	Vehicle Identifiers
Device IDs, Serial #	URLs	IP addresses
Biometric info	Photos	Any unique identifying info

REMEMBER: Minimum Necessary – must always use /disclose the least amount of information necessary / appropriate.

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: OTHER REQUIREMENTS RELATED TO USE AND DISCLOSURE

Fundraising Communications – if notice is given in Notices of Privacy Practices, can disclose to BAs or related Foundation

Verification Requirements – need to verify the entity/person requesting access to PHI is who they claim to be / have the authority (i.e administrator of estate)

Can rely on identity of public official if reasonable:

sheriff deputy with proper badge, in uniform

a written request on official state letterhead

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: NOTICE OF PRIVACY PRACTICES (NOPP)

Individuals have right to have notice of CE's privacy practices

Several required elements in the Notice

Must indicate if CE will do fundraising, give individual opportunity to opt out

Must Give Individuals Notice of:

- Their rights & how to exercise those rights
- The CE's obligations
- The right to, and information on how to, file a complaint
- The right to get more information, and how to get it
- The effective date of the notice

If NOPPs materially change, must provide new notice before effective date

Must provide at initial enrollment , and no less than every three years thereafter

Can post to website, but must be prominently **located**

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: INDIVIDUALS RIGHTS IN THEIR PHI

Request for restriction of uses and disclosures:

- Individual can request disclosure limited to only TPO - or -
- Individual can request limit to family / friends involved in care
- CE does not have to agree to request unless Individual obtains medical care and pays cash for it in full – can prevent disclosure to health plan

Request for confidential communications:

- CEs must accommodate reasonable request that CE communicate with individual by alternative means or alternative location
- CE may require request to be in writing
- CE can not require an explanation for the request

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: INDIVIDUALS RIGHTS IN THEIR PHI

Access to their PHI

- Individual has right to access to inspect and copy their PHI, except
  - psychotherapy notes
  - information compiled in anticipation of litigation
- CEs can deny request under certain conditions
- Denial can be reviewed in some cases
- CE can require request be in writing
- CE has 30 days to provide, or may invoke a one time 30 day extension
- Must provide in form (electronic, hard copy) requested if reasonable
- Can charge a reasonable cost-based fee
- Can redact some information under certain conditions

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: INDIVIDUALS RIGHTS IN THEIR PHI

Amendment of Individual's PHI

- CEs may deny if PHI was not created by CE or is accurate and complete
- CE may require request be in writing
- CE must act within 60 days of request, one 30 day extension available
- If CE denies request to amend, must give written explanation why
- Individual has opportunity to include a rebuttal statement in records

Accounting of Disclosures

- CE must provide accounting of disclosures for past 6 years, with certain exceptions (i.e. disclosures to individual, TPO, pursuant to a release, etc)
- Required contents of accounting: date, to whom, purpose, PHI disclosed
- CE must act within 60 days of request, one 30 day extension available

ROCKY MOUNTAIN HEALTH PLANS®
We understand Colorado. We understand you.

HIPAA PRIVACY: ADMINISTRATIVE REQUIREMENTS

CEs must :

- designate a Privacy Official
- train their workforce on the CE's P&Ps
- must have administrative, technical, and physical safeguards in place to protect the privacy of PHI
- provide process for complaints and document all complaints
- must have and apply appropriate sanctions for worker's violations
- must mitigate any harmful effects from violations
- not intimidate, threaten, coerce, discriminate against anyone for exercising their rights
- not require a waiver of any rights
- change it's P&Ps and NOPP when appropriate and necessary
- maintain documentation for 6 years