NEVADA HEALTH AUTHORITY

HIPAA Overview

May 21, 2026

www.pebp.nv.gov

WHAT IS HIPAA?

Health Insurance Portability and Accountability Act

- **42 U.S.C. § 1320d et seq.**
- **45 C.F.R. Parts 160 and 164**

PEBP is a “Covered Entity” Subject to HIPAA

Covered entities:

- Health plans (includes group health plans that pay the cost of medical care);
- Health clearinghouses:
- Health care providers who transmit health information in electronic form

(45 C.F.R. § 160.103)

PEBP Board and HIPAA

May learn protected health information in carrying out Board duties

Awareness of PEBP policies for staff who frequently deal with PHI

Focus: Privacy Rule

Prohibits unauthorized disclosure of protected health information (PHI)

- PHI is *individually identifiable health information* held or transmitted by a covered entity in any form or media (i.e., electronic, paper, verbal) that relates to:
  - Past, present, or future physical or mental health or condition,
  - Provision of health care, or
  - Past, present, or future payment for health care,
    and that identifies the person (or could reasonably be used to identify the person), such as name, address, birth date, Social Security Number.

- For example: claim information, EOBs, enrollment info

(45 C.F.R. Part 160 and Part 164, Subparts A and E)

Permitted Uses and Disclosures

(not all inclusive)

- Treatment, payment, and health care operations
- When required by law
- Public Health Activities

KEY: Minimum Necessary

Security Rule

Protects electronic PHI

- Administrative policies
  - Ex.: Personnel screening, access management, training
- Physical access controls
  - Ex.: Work station access, passwords
- Technical security measures
  - Backup, when to encrypt

(45 C.F.R. Part 160 and Part 164, Subparts A and C)

Examples of PEBP safeguards

- Key card access to areas where PHI may be
- Visitor procedures
- Passwords
- Shredding
- Login monitoring
- Anti-virus/anti-malware software
- Encrypted computer files
- Locked drawers and file cabinets
- Use of secure transfer sites

Examples of PEBP safeguards cont'd

- Designated privacy officer/contact person
- Complaint procedure
- Biennial compliance assessment includes review of HIPAA compliance
- Staff HIPAA training (initial and annual), with records maintained
- Provide Notice of Privacy Practices to plan participants (recently updated)

Breach Notification Rule

In event of data breach, covered entity must notify affected individuals and relevant authorities

(45 C.F.R. §§ 164.400-.414)

HITECH

Health Information Technology for Economic and Clinical Health Act

Enacted 2009 (13 years after HIPAA)

Promoted adoption of electronic health records

Strengthened HIPAA compliance requirements

- Extended HIPAA requirement to business associates of covered entities
- Tougher penalties for violating HIPAA

Business Associates

- Most of PEBP's vendors are business associates subject to HIPAA requirements
- Business associate agreements setting forth HIPAA requirements are part of contracts

Risks of noncompliance

Civil: Monetary penalties, corrective action plans

Criminal: For intentional breach of PHI, fines and imprisonment

(HIPAA Enforcement Rule: 45 C.F.R. Part 160, Subparts C, D, and E)

Anthem settlement

- Cyber-attackers gained access to databases through phishing emails sent to Anthem subsidiary
  - “At least one employee responded to the malicious email and opened the door”
- In approximately two months, cyber-attackers stole ePHI or almost 79 million persons
  - Names, social security numbers, medical ID numbers, addresses, DOBs, email addresses, and employment information
- Anthem reported breach to U.S. Department of Health and Human Services Office for Civil Rights (OCR)
- Anthem faced investigations by most state attorneys general, class action lawsuit, and enforcement action by OCR
- While maintaining that it did not violate the law and that no evidence supported that any of the stolen information was used to commit fraud of identity theft, Anthem agreed to pay $16 million to OCR and take substantial corrective action to settle enforcement matter

Cadia Healthcare Facilities settlement

- 2025 settlement with OCR for potential HIPAA violations
- Complaint asserted that Cadia impermissibly disclosed patient's name, photo, and information pertaining to patient's conditions, treatment, and recovery as a "success story" on website
  - Failed to obtain HIPAA authorization form before doing so
  - OCR investigation showed similar pattern for 150 patients
- Failed to comply with Breach Notification Rule by failing to inform affect persons
- Agreed to corrective action plain and $182,000 penalty

Questions/discussion?