HIPAA Security Guidelines

3 key safeguards:

Physical Safeguards:

this protects the physical security of their offices where PHI or ePHI may be stored or maintained. Some examples are: alarm systems, security systems, locking areas where PHI is stored.

Technical Safeguards:

this protects ePHI from the threat of cyberattacks. Some examples include: firewalls, data encryption, and data backup.

Administrative Safeguards:

this ensures that staff members are properly trained to execute the security measures you have in place. These safeguards should include policies and procedures that document the security safeguards you have in place, as well as employee training on those policies and procedures.

Addressing HIPAA Cybersecurity

HIPAA regulation developed strict guidelines for standards that must be carried out in order to keep protected health information (PHI) secure.

> "The Cottage settlement reminds us that information security is a dynamic process and the risks to ePHI may arise before, during, and after implementation covered entity makes system changes."

– Roger Severino, OCR Director

The guidance identifies the following ten practices to alleviate the most impactful cybersecurity threats:

Email protection systems

Endpoint protection systems

Access management

Data protection & loss prevention

Asset management

Network management

Vulnerability management

Incident response

Medical device security

Cybersecurity policies

NovaBACKUP

29209 Canwood Street
Agoura Hills, CA 91301
(805) 579-6700
msp@novabackup.com

Compliancy Group

HIPAA SEAL OF COMPLIANCE — COMPLIANCY GROUP — HIPAA VERIFIED