NovaBACKUP
HIPAA Safeguards Document

What specific HIPAA safeguards do NovaBACKUP products support?

The HIPAA Security Rule lays out three types of safeguards required for compliance: **administrative**, **physical**, and **technical**.

HIPAA rules apply to doctors, clinics, psychologists, dentists, chiropracters, nursing homes, pharmacies, health insurance companies, HMOs and more. These covered entities are required to protect the privacy and security of health information. Part of that protection involves having a contingency plan on how to continue operations in the event a data loss, including details regarding their data backup and recovery process. These organizations must document safeguards for everything from who handles the backup media and rotation process, to where media is stored offsite, to how media is disposed of, to how quickly data can be retrieved in the event of a loss, to the encryption level used to protect health information.

Administrative Safeguards

Contingency Plan

1. Data Backup Plan (Required) ..... ☑
2. Disaster Recovery Plan (Required) ..... ☑
3. Emergency Mode Operation Plan (Required)
4. Testing and Revision Procedures (Addressable)
5. Applications and Data Criticality Analysis (Addressable)

NovaBACKUP allows you to create a comprehensive plan for the recovery of critical information. This includes extensive functionality for disaster recovery, capable of restoring your data — even to dissimilar hardware. A backup is only as good as your ability to recover, so testing your backups should be included in your testing proceedures.

Physical Safeguards

Device and Media Controls

1. Disposal (Required)
2. Media Re-Use (Required)
3. Accountability (Addressable)
4. Data Backup and Storage (Addressable) ..... ☑

NovaBACKUP allows for the backup of critical data to multiple locations for local and offsite backups and ensures that an exact copy is available prior to making changes to your network infrastructure.

Technical Safeguards

Access Controls

1. Unique User Identification (Required)..... ☑
2. Emergency Access Procedure (Required)
3. Automatic Logoff (Addressable)
4. Encryption and Decryption (Addressable) ..... ☑

Backup activity for specific users may be monitored from NovaStor's Central Management Console product which integrates seamlessly with all NovaBACKUP products.

NovaBACKUP provides you with a powerful tool for the encryption and decryption of data according to administrator specifications.

Audit Controls ..... ☑

NovaStor's Central Management Console allows you to monitor and examine user backup activity, as well as generate high quality reports for backup management.

Integrity ..... ☑

Person or Entity Authentication ..... ☑

Through the use of user verification, authentication and data encryption, NovaBACKUP ensures that your critical data remains protected and unaltered. By generating custom encryption keys specific to the user, data access is restricted.

Transmission Security

1. Integrity Controls (Addressable) ..... ☑
2. Encryption (Addressable) ..... ☑

In local and cloud backup scenarios, NovaBACKUP utilized end-to-end 256-bit AES encryption for file and image backups.

About HIPAA

For complete information on the HIPAA Security rule and safeguards required for compliancy, please visit the HHS website:

www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Contact your dedicated NovaStor sales specialist to receive pricing and product recommendation for your environment:

U.S. Tel: +1.805.579.6700
onlinesales@novastor.com

NOVASTOR

www.novabackup.com

NovaStor Software AG
Baarerstrasse 20
CH-6304 Zug
Tel +41 (41) 712 31 55
Fax +41 (41) 712 31 56

NovaStor Corporation
29209 Canwood Street
Agoura Hills, CA 91301 USA
Tel +1 (805) 579 6700
Fax +1 (805) 579 6710

NovaStor GmbH
Neumann-Reichardt-Str. 27-33
D-22041 Hamburg
Tel +49 (40) 638 09 0
Fax +49 (40) 638 09 29