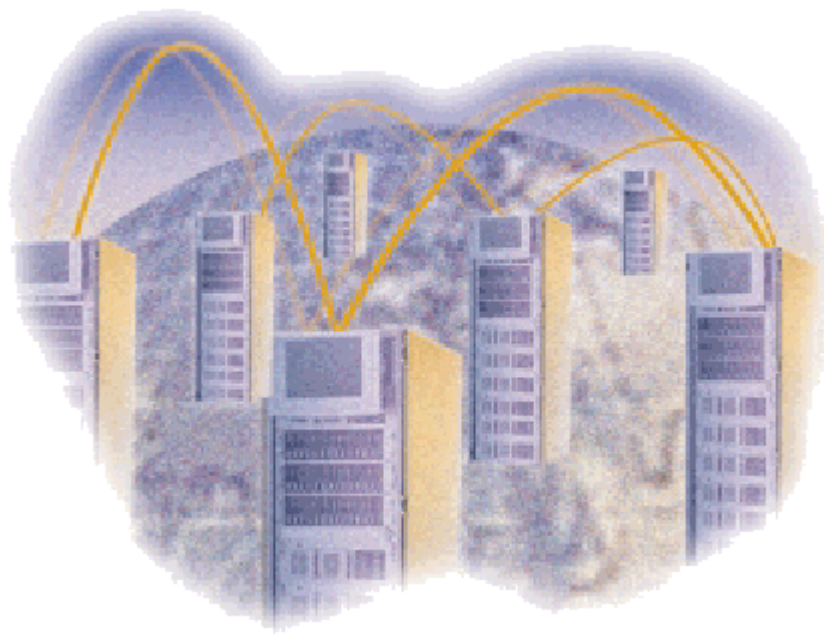




Double-Take in a HIPAA Regulated Health Care Industry



Abstract: This document addresses the contingency plan and physical access control requirements of the Administrative Simplification security provision of HIPAA. It will assist health care providers (doctors, hospitals, pharmacies, health insurers, clearinghouses (third party vendors who convert data from paper to electronic), or any other organization directly handling patients' health care information) in recognizing how NSI Software's Double-Take can be implemented to fulfill these requirements.

NSI and Double-Take are registered trademarks of Network Specialists, Inc. All other products are trademarks of their respective companies.
© 1996–2002 NSI Software

Double-Take in a HIPAA Regulated Health Care Industry, published September 2002



Department of Health
and Human Services

Doctors, hospitals, pharmacies, health insurers, and other health care related entities process and track billions of health care bills, records, and other transactions. With so many different types of health insurance, doctors and hospitals must spend time and money ensuring that claims processed electronically contain the format and content required by each insurer. Additionally, health insurers spend time and money to ensure their systems can handle electronic transactions from numerous health care providers. Uniform national standards would save the health care industry billions of dollars by lowering the costs of developing and maintaining software and reducing the time and expense needed to handle electronic health care transactions.

The Health Insurance Portability and Accountability Act (HIPAA) enacted by the United States Congress in 1996 included a wide variety of provisions designed to make health insurance more affordable and accessible by establishing federal standard formats and data content for electronic transactions between all health care providers. One section of HIPAA, Administrative Simplification, has multiple parts - transactions standards and code sets, electronic signatures, security, privacy, and unique health identifiers. Focusing just on the Administrative Simplification security provision, HIPAA requires the development and implementation of administrative, technical, and physical safeguards to ensure the security of electronic transactions containing patients' health information.¹ These safeguards include contingency planning and physical access controls. Each security safeguards has required implementation steps including, but not limited to, disaster recovery, emergency mode operation, data backup, access restrictions, etc.²

It is with these security implementation steps that the right software application can simplify and ease the strategy for becoming HIPAA compliant. Keep in mind that some vendors may advertise solutions that can make a provider HIPAA compliant. But software, hardware, or a technical specification cannot determine compliance. Software can be only one mechanism for instituting the broad spectrum of HIPAA compliance.

NSI Software's Double-Take can fulfill the disaster recovery, backup, emergency mode operations, etc. duties that are required for HIPAA security implementation. Double-Take is a real-time data replication and failover



application that augments an existing network environment by providing a data protection mechanism that has minimal impact on users or network resources.

Double-Take allows the administrator to specify mission critical data, in this case patients' health records, stored on a network server and transmit that data to a second network server. Double-Take then monitors any changes to the data on the first server and replicates only those changes to the second server. The second server is synchronized with the first, therefore, data is protected and an up-to-date copy of the data is available.

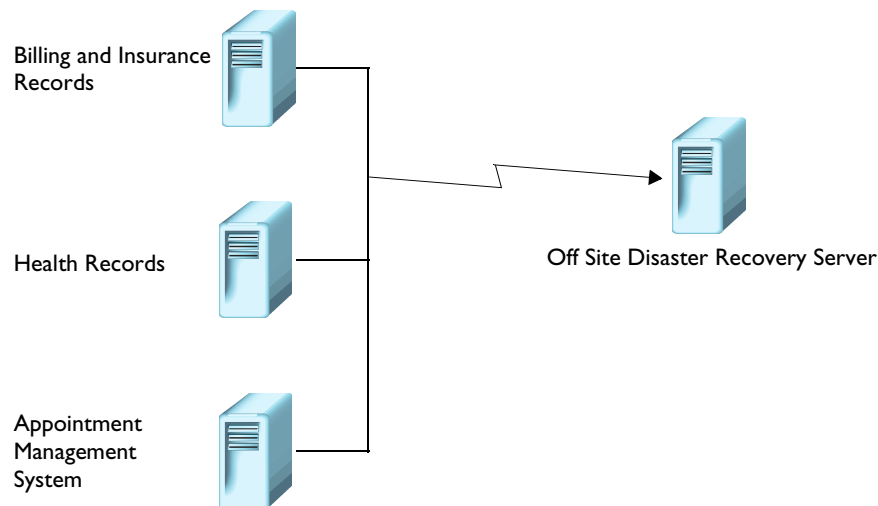
What does that mean to a health provider? Let's take a look at several of the Administrative Simplification security provisions in closer detail.

-
1. The words security should not be confused with either privacy or confidentiality. Privacy refers to the rights of an individual to control his personal information and not to have it divulged or used by others against his wishes. Confidentiality is a means of protecting an individual's personal information from unauthorized disclosure after the information has been received by another entity. Security applies to the actual physical, technical, and administrative safeguards that are put in to place to protect the integrity, availability, and confidentiality of information.
 2. For a complete listing of all of the requirements and the mandatory implementation steps to meet each requirement, see the Security and Electronic Signature Standards rule published by the Department of Health and Human Services at <http://aspe.hhs.gov/admsimp/bannerps.htm#security>.

Administrative Contingency Plan—The administrative safeguards “require a contingency plan to be in effect for responding to system emergencies. The organization is required to perform periodic tape backups of data, have available critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place.”³ Double-Take automates some of these processes by providing a disaster recovery implementation that saves time and resources.

Say for example, you have multiple servers that contain patient records. These servers are known as your production servers because these records are the main files that are updated by your personnel. To implement a disaster recovery process, you need another server, located off site, that contains an exact copy of the data on the production servers. Unlike backup technologies which create only a daily or weekly copy of the data, Double-Take is designed to create and maintain an up-to-the-minute copy of the data on your production servers. Even if your office is smaller with only one server, you still need a disaster recovery plan in order to comply with the contingency plan. In the case of a smaller office, the configuration might have only one or two production servers but would be implemented in the same way.

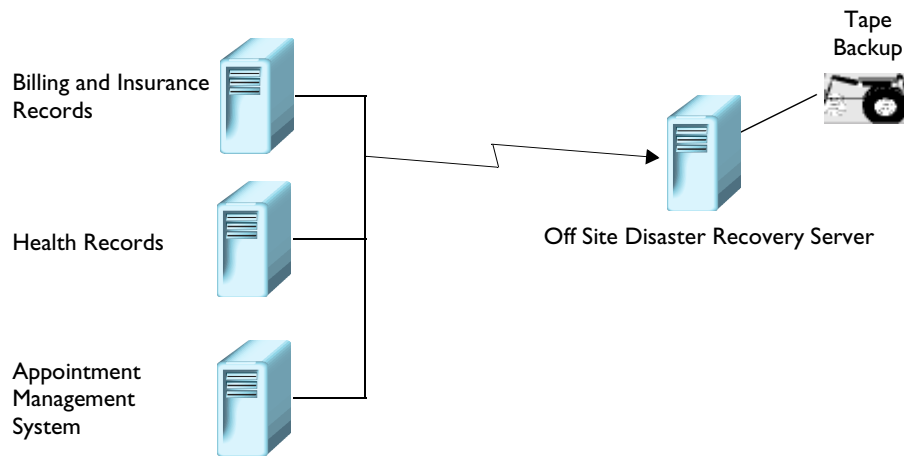
Off Site Disaster Recovery



3. Department of Health and Human Services, Office of the Secretary, 45 CFR Part 142, Security and Electronic Signature Standard.

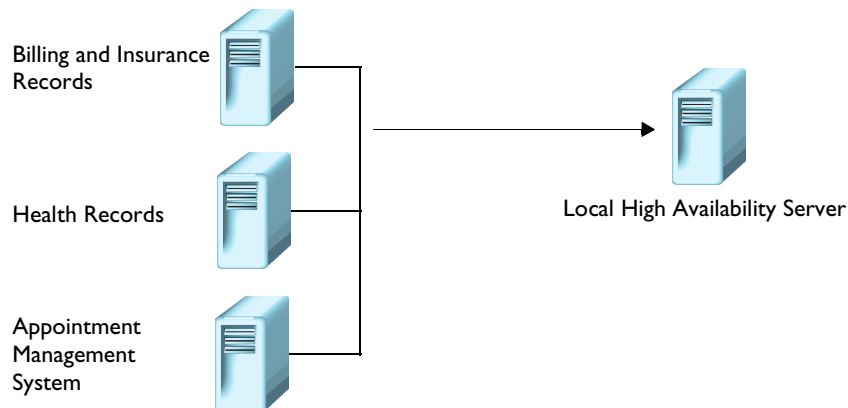
The administrative contingency plan also calls for a data backup plan. While Double-Take is not a data backup solution, it can enhance an existing backup solution. Unlike tape backups which run periodically to provide archival data, Double-Take continuously captures the most recent data and makes it immediately available. This allows the backup duties, which can often be detrimental to system performance, to be relocated off of the production machines and away from users to the disaster recovery server where the performance impact is less significant.

Off Site Disaster Recovery With Data Backup



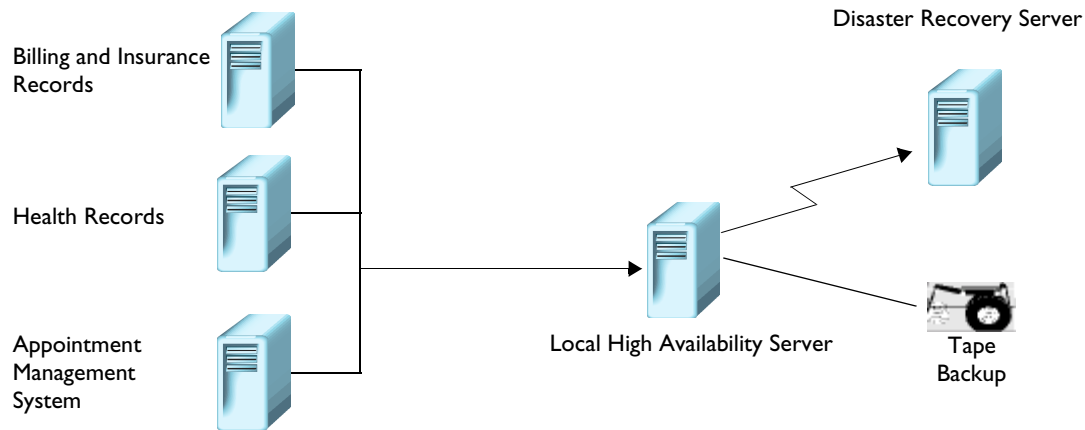
A third implementation requirement of the administrative contingency plan is an emergency mode operation plan. Your office needs to be able to continue functioning in the event of an emergency. With Double-Take an up-to-date copy of the production data is always available on the disaster recovery server. But you can go even further with Double-Take by adding high availability to your contingency plan. In the event that a production server fails, Double-Take can seamlessly move, or failover, the responsibilities and roles of the failed server to the high availability server because it contains an exact replica of the production data. Users can access the high availability server as if it was the production machine. In the event of an emergency, your data would not only be protected but would be accessible within minutes.

Emergency Mode Operation (Local High Availability)



Double-Take's flexibility allows you to combine these configurations to suit your needs. Perhaps you would want a local high availability server with a tape backup and an off site disaster recovery plan. Double-Take can implement these solutions easily.

Local High Availability With Data Backup and Off Site Disaster Recovery



Physical Access Controls—The physical safeguards require “limiting physical access to an entity while ensuring that properly authorized access is allowed.”⁴ The same implementation requirements (disaster recovery, data backup, and emergency mode operation) are again mandatory. While the physical aspects of security are unique to every building and physical environment, Double-Take also has access controls in place. Double-Take builds on the proven reliability of Microsoft by using native Windows operating system security features. As long as proper security processes are in place (such as physical restriction to servers, proper Windows security policies and procedures, and other HIPAA security requirements), Double-Take will compliment the access restrictions required for HIPAA compliance.⁵

Double-Take offers many other features and benefits that can enhance and optimize the environment used by large or small health care providers. Engage NSI Software Professional Services to realize the full potential of Double-Take. They can deliver a comprehensive portfolio of services to help assess, design, plan, and implement effective data availability and disaster recovery solutions. For questions on Double-Take, including pricing and product features call NSI Software's toll free number 888-674-9495 or send e-mail to info@nsisoftware.com.

4. Department of Health and Human Services, Office of the Secretary, 45 CFR Part 142, Security and Electronic Signature Standard.
5. For detailed information from Microsoft concerning HIPAA implementation, see www.microsoft.com/solutions/HIPAA/techinfo/healthinformation.asp.