UCG Technologies is the data protection expert, trusted by healthcare organizations of all sizes. Since 1987, we have delivered easy-to-use solutions that keep data secure and immediately recoverable while controlling costs. Our disk-to-disk backup and recovery technology, coupled with consulting and educational services, provides you with data protection that helps assure compliance with the Health Insurance Portability and Accountability Act (HIPAA).

High performance backup and recovery
The increasing complexity of your IT environment, especially the hyper-growth of data and applications, makes it essential that your backup and recovery system is at once high-performing, easy to configure, and easy to use. UCG’s VAULT400 Cloud Backup & DRaaS provides that in a unified solution that integrates with your systems seamlessly and scales readily as you grow. VAULT400 backs up your core systems, networked environments, and mobile devices wherever they are, and no matter how complex.

Eliminate compliance concerns
All of our data centers complement a variety of industry and government mandates including HIPAA, PCI DSS and SOX, supported by third-party SSAE 16/SOC attestation reports.

To comply with HIPAA, your organization must securely back up data, retain disclosures, provide physical and technical safeguards, and ensure disaster recovery. UCG’s data protection platform simplifies this, with uncompromising performance, brilliant simplicity and a comprehensive breadth of application and platform support.

The technology behind VAULT400 Cloud Backup & DRaaS has enabled the safekeeping of more than 40% of the world’s digital information.
HIPAA Implications for Data Retentions Addressed

<table>
<thead>
<tr>
<th>Policies and Procedures</th>
<th>Offsite Storage</th>
<th>Data Availability</th>
<th>Security and Privacy</th>
<th>Retentions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documented backup and recovery plan</td>
<td>Patient-pending delta-processing technology enables high performance WAN/LAN backup and recovery and optimizes storage</td>
<td>Immediate file and folder-level recovery</td>
<td>NIST-certified AES Encryption End-to-End</td>
<td>Policy-based automated retentions you set based on your needs</td>
</tr>
<tr>
<td>Emergency contingency planning</td>
<td></td>
<td>File search to support regulatory audits</td>
<td>SAS 70 certified</td>
<td>File level archiving</td>
</tr>
<tr>
<td>Log reports</td>
<td>Disaster Recovery testing</td>
<td>Disaster recovery strategies and specialized services</td>
<td>Disk-based storage—no tape-based risk</td>
<td>Email and IM backup and archiving</td>
</tr>
</tbody>
</table>

HIPAA Compliance Checklist

**Rule on Security Standards: Administrative Safeguards**

*Data Backup and Disaster Recovery*
Covered entities are responsible for backing up their data and establishing disaster recovery procedures. A contingency plan should be in place for responding to emergencies.

*Privacy Rule: Retention of Disclosures*
Covered healthcare entities must keep track of disclosures of Protected Health Information (PHI) for a period of six years. This includes any part of a patient’s medical record or payment history.

**Rule on Security Standards: Administrative Safeguards**

*Access to Records*
Access to Electronic Protected Health Information (EPHI) must be restricted to only those employees who have a need for it to complete their job function.

**Rule on Security Standards: Administrative Safeguards**

*Outsourcing*
Covered entities that outsource some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements.

**Rule on Security Standards: Physical Safeguards**
Access to equipment containing health information should be carefully controlled and monitored, based on facility security plans, maintenance records, and visitor sign-in and escorts.

**Rule on Security Standards: Technical Safeguards**
When information flows over open networks, some form of encryption must be utilized.

**UCG’s technology includes encryption in storage, as well as during transmission. Original versions of documents, once backed up, cannot be accessed except by authorized personnel. Data is encrypted before it leaves the firewall and remains that way. Not even UCG can access your information.**

**UCG data centers complement a variety of industry and government mandates including HIPAA, PCI DSS and SOX, supported by third-party SSAE 16/SOC attestation reports.**

**At our offsite data centers, security and availability of organization’s data meet the highest industry standards. Access is strictly limited and enforced.**

**UCG’s AES encryption technology is NIST certified. It meets or exceeds all regulatory requirements including HIPAA.**

**UCG provides secure, reliable online data protection. Tape-based risk is eliminated. You never lose your data. UCG’s Professional Services consultants help you develop a data protection strategy that assures you meet compliance requirements. This information is documented and delivered in a comprehensive data protection plan.**

**UCG’s ArcWare is a policy-based archiving solution that lets you move older files off production servers and store them in a Vault. Tiered storage strategies let you optimize production space.” UCG’s ProMail ensures your important electronic messages are safe and accessible. It captures, monitors, and archives email and instant messages up to seven years, and makes it easy to satisfy your retention policies.**

UCG Technologies
7100 E. Pleasant Valley Road, Suite #250
Independence, OH 44131-5556

800.211.8798 • info@ucgtechnologies.com

ucgtechnologies.com