CyberHealth Solutions - Data Breach Response Plan

# 1. Purpose

To outline the procedures for responding to data breaches involving Protected Health Information (PHI) and other sensitive data.

# 2. Scope

This plan applies to all employees, contractors, and associates of CyberHealth Solutions.

# 3. Breach Definition

A data breach is any unauthorized acquisition, access, use, or disclosure of sensitive data that compromises the security or privacy of such information.

# 4. Response Team

The Data Breach Response Team includes:  
- Privacy Officer  
- IT Security Lead  
- Legal Advisor  
- Communication Officer

# 5. Response Procedures

Step 1: Identification and Containment  
- Detect and contain the breach.  
- Document initial findings.  
  
Step 2: Notification  
- Notify internal stakeholders immediately.  
- Report the breach to HHS OCR within 60 days if PHI is affected.  
  
Step 3: Investigation and Impact Assessment  
- Determine the scope of the breach.  
- Identify affected individuals and data types.  
  
Step 4: Remediation and Recovery  
- Implement corrective actions.  
- Restore data and system integrity.  
  
Step 5: Documentation and Reporting  
- Complete an incident report.  
- Retain records for 6 years.

# 6. Training and Testing

All staff must receive annual training on breach response. Simulated breach drills should be conducted annually.

# 7. Contact Information

Privacy Officer: privacy@cyberhealth-solutions.com  
IT Security: security@cyberhealth-solutions.com