# Security Information

Last Updated: August 1, 2025

## Our Commitment to Security

At Friendly Care LLC, we take the security of your personal information seriously. This page outlines the technical, administrative, and physical safeguards we implement to protect your data and ensure the security of our services.

## Data Security Framework

### Technical Safeguards

Encryption

* All data transmitted to and from our website uses SSL/TLS encryption (minimum TLS 1.2)
* Sensitive data stored in our databases is encrypted at rest using industry-standard encryption
* Payment information is processed through PCI-compliant payment processors
* Email communications containing sensitive information are encrypted

Access Controls

* Multi-factor authentication (MFA) required for all administrative accounts
* Role-based access controls limit data access to authorized personnel only
* Regular access reviews and permission audits
* Automatic session timeouts to prevent unauthorized access

Network Security

* Firewalls and intrusion detection systems monitor network traffic
* Regular vulnerability assessments and penetration testing
* Secure configuration of servers and applications
* Network segmentation to isolate sensitive systems

Application Security

* Secure coding practices and regular code reviews
* Input validation and sanitization to prevent injection attacks
* Regular security updates and patches
* Web application firewalls to filter malicious traffic

### Administrative Safeguards

Personnel Security

* Background checks for employees with access to personal information
* Regular security awareness training for all staff
* Confidentiality agreements and privacy training
* Clear incident response roles and responsibilities

Policies and Procedures

* Comprehensive information security policies
* Regular policy reviews and updates
* Documented security procedures and protocols
* Change management processes for security controls

Monitoring and Auditing

* Continuous monitoring of systems and data access
* Regular security audits and assessments
* Log management and analysis
* Compliance monitoring and reporting

### Physical Safeguards

Facility Security

* Restricted access to data centers and office facilities
* Security cameras and alarm systems
* Visitor management and escort procedures
* Environmental controls to protect equipment

Device Security

* Encrypted laptops and mobile devices
* Remote wipe capabilities for lost or stolen devices
* Secure disposal of hardware containing data
* Cable locks and physical security for workstations

## Data Protection Measures

### For Job Applicants

* Application data is stored in secure, access-controlled systems
* Resume and personal information are protected with encryption
* Background check information is handled according to FCRA requirements
* Data retention follows employment law requirements

### For Service Clients

* Care-related information is protected with healthcare-level security
* Personal care preferences and schedules are encrypted
* Emergency contact information is securely stored and readily accessible to authorized caregivers
* Service notes and documentation are access-controlled

### For Website Visitors

* Browsing data is anonymized where possible
* Contact form submissions are encrypted in transit
* Marketing data is stored securely and access-controlled
* Cookie data is handled according to our Cookie Policy

## Incident Response

### Detection and Response

We maintain a comprehensive incident response plan that includes:

* 24/7 monitoring for security threats
* Automated alerting for suspicious activities
* Rapid response team activation procedures
* Forensic analysis and containment measures

### Notification Procedures

In the event of a data breach:

* We will investigate and assess the scope within 24 hours
* Affected individuals will be notified within 72 hours (or as required by law)
* Relevant authorities will be notified as required
* We will provide ongoing updates as the investigation progresses

### Recovery and Prevention

* Immediate steps to contain and mitigate the incident
* System restoration and data recovery procedures
* Analysis of root causes and security improvements
* Updated training and procedures to prevent recurrence

## Compliance and Certifications

### Industry Standards

We align our security practices with recognized frameworks:

* NIST Cybersecurity Framework
* ISO 27001 information security standards
* HIPAA Security Rule principles (for health-related data)
* PCI DSS requirements for payment processing

### Regular Assessments

* Annual third-party security assessments
* Quarterly internal security reviews
* Ongoing vulnerability scanning and testing
* Regular penetration testing by certified professionals

### Compliance Monitoring

* Continuous compliance monitoring and reporting
* Regular updates to security controls based on new threats
* Documentation of security measures for regulatory purposes
* Staff certification and training programs

## Third-Party Security

### Vendor Management

* All service providers undergo security assessments
* Contractual requirements for data protection and security
* Regular monitoring of third-party security practices
* Incident notification requirements from vendors

### Integration Security

* Secure APIs and data exchange protocols
* Regular security testing of third-party integrations
* Monitoring of data flows to and from external systems
* Documented security requirements for all integrations

## Your Role in Security

### Account Security

* Use strong, unique passwords for your accounts
* Enable two-factor authentication when available
* Log out of shared or public computers
* Report suspicious account activity immediately

### Communication Security

* Verify the authenticity of communications claiming to be from us
* Do not share personal information via unsecured channels
* Be cautious of phishing attempts and suspicious links
* Contact us directly if you receive suspicious communications

### Device Security

* Keep your devices updated with latest security patches
* Use reputable antivirus software
* Secure your home WiFi network
* Be cautious when using public WiFi for sensitive activities

## Reporting Security Issues

### How to Report

If you discover a security vulnerability or incident:

Email: security@yourfriendlycare.com
 Subject Line: Security Issue - [Brief Description]

Include:

* Detailed description of the issue
* Steps to reproduce the vulnerability
* Potential impact assessment
* Your contact information for follow-up

### Response Timeline

* Acknowledgment within 24 hours
* Initial assessment within 72 hours
* Regular updates during investigation
* Resolution notification once issue is addressed

### Responsible Disclosure

We appreciate responsible disclosure of security issues and commit to:

* Working with researchers to understand and fix issues
* Providing timely updates on remediation progress
* Recognizing researchers who help improve our security (with permission)
* Not pursuing legal action against good-faith security research

## Security Updates and Improvements

We continuously improve our security measures through:

* Regular security training for all employees
* Investment in new security technologies
* Participation in industry security initiatives
* Collaboration with security experts and researchers

## Contact Us

For security-related questions or concerns:
 General Inquiries: info@yourfriendlycare.com

Friendly Care LLC
 Phone: (860) 382-4625

*This Security Information page is updated regularly to reflect our current security practices and should be reviewed periodically.*