Security and Encryption Considerations for a Dementia Support and Geofencing Application

Developing an application to help individuals with early-onset dementia requires a careful balance between promoting independence and ensuring safety. A geofencing system that alerts caregivers when a user leaves a preset boundary involves ongoing location tracking, careful data handling, and secure communication methods. This group is vulnerable, so any misuse or data breach can have serious ethical and safety consequences. This expanded document offers more details on encryption methods, security needs, privacy standards, design focused on mental capacity, and other technical and ethical issues.

1. Core Encryption Methods

Data-in-Transit Encryption- Data transmitted between the mobile device, backend server, and carer dashboard must be encrypted end-to-end.
Transport Layer Security (TLS 1.3) provides:
Forward secrecy: Session keys are not reused, preventing previously captured traffic from being decrypted.
Reduced handshake steps: Improved performance and security for frequent location updates.
Modern cipher suites only: Removes support for older, vulnerable algorithms.

Possible Additional considerations:
Use HSTS (HTTP Strict Transport Security) to ensure clients cannot downgrade to insecure connections.
Implement certificate pinning so the app only trusts your server's certificate, blocking forged certificates.
Avoid exposing unnecessary APIs—limit endpoints to essential operations to reduce attack surface.

Data-at-Rest Encryption - Information stored on servers, databases, or devices must be protected against unauthorised access.
AES-256 still remains the recommended standard due to:

- Resistance to brute-force attacks.
- Wide hardware support.
- Compatibility with secure key management frameworks.

To enhance protection:

- Implement server-side encryption with managed keys, such as AWS KMS or Azure Key Vault.
- Use device-level encryption (iOS File Protection / Android Full Disk Encryption) so stolen devices cannot reveal sensitive data.
- Store cryptographic keys separately from encrypted data.

Secure Hashing for Authentication - Secure password storage is essential. Using hashing algorithms such as Argon2, bcrypt, or PBKDF2 ensures:

- Strong resistance to brute-force attempts due to computational cost.
- Salted hashing prevents identical passwords from producing identical hashes.

Other considerations to bare in mind::
Implementing rate limiting and lockout policies to hinder automated guessing.
Using OAuth2 or OpenID Connect for carers who already use organisational identities.

2. Additional Security Measures

Multi-Factor Authentication for Carers. Carers access highly sensitive information that could be misused if compromised. MFA could include:

- Something they know (password).
- Something they have (authenticator app, hardware key).
- Something they are (fingerprint/FaceID).

This ensures that even if login credentials are leaked, unauthorised access remains highly unlikely

.
Endpoint Security - The app must protect itself from tampering.
Critical measures:

- Root/jailbreak detection to disable operation on insecure devices.
- Code obfuscation to protect sensitive logic from reverse engineering.
- Secure local storage: never store tokens or private keys in plain text.
- Automatic session timeout to prevent unauthorised access if a device is left unlocked.

Secure API Design- Our API should follow zero-trust principles.
Good practice includes:

- Role-based access control restricting what carers, admins, and users can view or modify.
- Implement rate limiting to prevent enumeration or brute-force attacks.
- Use opaque identifiers instead of incremental database IDs.
- Validate all inputs to prevent injection attacks.

Minimal and Ethical Data Retention - keep only what data is required to fulfil the purpose.
Recommendations:

- Automatically purge location data after a configurable time frame.
- Provide carers and users with deletion controls.
- Avoid storing continuous real-time location history unless required.
- Use anonymisation techniques for system analytics.

3. Privacy Considerations

Data Minimisation Principles - The app should collect only essential information, such as: Geofence boundaries.
What data we might need:

- Real-time location (only when needed for safety).
- Contact details for carers.

What we don't need but is picked up if our data collection isn't precise:
Continuous medical metrics
Unnecessary background data like Bluetooth logs or app usage.

Transparency and User Rights - Users should receive clear and simple explanations. This may include:

- Plain-language summaries of data practices.
- Icons or colour-coded explanations of what is shared.
- Clear toggles for optional data categories. (such as only collecting route data if ai mode is enabled)
- Easy-to-trigger information requests under GDPR or equivalent regulations.

Compliance With Regulations,depending on the region, compliance with GDPR, HIPAA (if medical data is stored), or local safeguarding laws is essential.(only important if app is used outside of UK)
This complicates data handling because:

- Location data is legally recognised as sensitive.
- Consent must be informed, meaningful, and freely given.
- Users can revoke consent at any time.

4. Mental Capacity and Consent-Focused Design

People with early-onset dementia often retain capacity, especially during early stages. Our app design should:

- Recognise fluctuating capacity.
- Provide the user with as much autonomy as possible.
- Allow users to review—and re-review—permissions over time.

Ethical Consent Features - the app can incorporate:
Periodic reconfirmation prompts (e.g., every 3–6 months).
Tiered understanding checks, such as: “Do you understand that your location is shared with people you trust?”
Consent recording, documenting who provided consent and when.

In cases where the user lacks capacity, local legal frameworks (e.g., the UK Mental Capacity Act 2005) specify that decisions must be made in their best interests.

Designing the app to feel empowering rather than controlling assists in clear understanding:

- Avoid language that suggests surveillance.
- Provide reassurance-based notifications.
- Encourage independence by letting users set their own comfort zones where feasible.

Carer Responsibilities - Carers must be educated on privacy obligations.Important that we ensure they understand how to use data appropriately.

5. Threat Scenarios and Mitigation

Unauthorised Access or Account Hijacking - If a bad actor gains access to a carer's account, they could track a vulnerable person.
Solutions: MFA , Behaviour-based anomaly detection , Automatic notifications for new login devices.

Device Loss or Theft. Because our users might misplace devices more often we should provide remote lock/wipe capabilities and ensure all sensitive data remains behind device-level encryption.Addtionally, notify carers immediately when the device stops communicating.

Server-Side Breaches - Mitigations include:

- Segregated databases for identity and location.
- Encryption of sensitive fields at the application layer.
- Frequent penetration testing.
- Routine vulnerability scanning.

Malware or Rogue Apps- To reduce the risk:

- Use app attestation services like Google Play Integrity API or Apple DeviceCheck.
- Prevent the app from running on insecure operating system versions.

GPS Spoofing or Location Tampering- A malicious actor could try to spoof a location.
Countermeasures:

- Detecting abnormal GPS behaviour.
- Use multiple location sources (GPS, Wi-Fi, cell tower triangulation).
- Validate impossible movement speeds.

6. Ethical Technology Use

Proportionality and Respect- Tracking should only occur for safety purposes.
Avoid:

- Real-time tracking when not necessary.
- continuous data collection unrelated to wellbeing