Human Research Ethics Application

Pilot Study: Wearable-Initiated Community Proximity Emergency Response Network

HREC Protocol Number: [TO BE ASSIGNED]

Version 3.0 — February 2026

Principal Investigator: [NAME]
Institution: [INSTITUTION]
Contact: research@omxus.com

Contents

1 Project Summary

1.1 Title

Civic Proximity Response: A Pilot Study of Wearable-Initiated Community Emergency Networks in Suburban Australia

1.2 Plain Language Summary

We want to test whether a simple wearable device (an NFC ring) can help people in emergencies get help faster from nearby community members, while ambulance and police services continue operating as normal.

Participants in one suburban community will receive an NFC ring and a smartphone app. If they experience or witness an emergency, they can tap the ring to send an alert to other participants nearby. Nearby participants who receive the alert can choose to respond by going to help, or not. The study measures how quickly someone arrives compared to traditional emergency services.

The ring does *not* replace Triple Zero (000). Participants are told to always call 000 for serious emergencies. The ring provides additional first-contact from community members during the minutes before professional help arrives.

The study will run for 12 months with approximately 500 adult participants.

1.3 Research Question

> Does a wearable-initiated community proximity alert system reduce median time-to-first-contact in emergency events, compared to centralised emergency dispatch alone, when operating as a supplementary layer alongside existing Triple Zero services?

1.4 Study Design

Type: Prospective observational cohort with historical control comparison.

Design: Single-arm deployment of the intervention (NFC ring + mesh alert network) with comparison against historical EMS response time data for the same geographic area from the preceding 24 months.

Rationale for single-arm: Randomisation (giving some participants rings and not others in the same community) would compromise the mesh density that the system requires to function. The system's value depends on network density; a randomised design would test the system under artificially degraded conditions.

1.5 Funding Source

[TO BE COMPLETED — self-funded / grant application / institutional support]

1.6 Conflicts of Interest

The research team includes members of the OMXUS project, which developed the technology being tested. This is a substantive conflict that we take seriously and manage through multiple independent safeguards:

1. **Independent DSMB:** An independent data safety monitoring board with authority to pause or terminate the study at any time. No DSMB member has any financial, employment, or advisory relationship with OMXUS.

2. **Pre-registered analysis plan:** The complete statistical analysis plan is registered with ANZCTR prior to first participant enrolment. No post-hoc changes to primary analysis are permitted without DSMB and HREC approval.

3. **Open data:** The complete de-identified dataset will be published at study completion regardless of results. Negative findings will be published with equal commitment.

4. **Independent statistical analysis:** Primary outcome analysis will be conducted by a statistician with no involvement in technology development, no financial relationship with OMXUS, and no prior knowledge of interim results.

5. **Negative results commitment:** The research team commits in writing to publishing results regardless of whether they support or undermine the technology's effectiveness. This commitment is recorded in the ANZCTR registration and forms a condition of ethics approval.

6. **No commercialisation during study:** No commercialisation activity (licensing, sales, investment solicitation) referencing pilot data will occur until final results are published and peer-reviewed.

7. **Investigator disclosure:** All investigators will disclose their relationship with OMXUS in every publication, presentation, and communication arising from this study.

Potential sources of bias and how they are addressed:

Bias Risk	Mechanism	Safeguard
Selection bias	Recruiting enthusiastic early adopters	Community-wide recruitment, not targeted at tech-enthusiastic populations
Measurement bias	Favourable interpretation of ambiguous outcomes	Primary outcome (time-to-contact) is objective and timestamped by device, not self-reported
Reporting bias	Suppressing negative results	Pre-registration, open data, negative results commitment
Social desirability	Participants over-reporting positive experiences in surveys	Anonymous surveys, objective app telemetry as primary data
Hawthorne effect	Behaviour change from study awareness	Single-arm design (all participants know); acknowledged as limitation

2 Ethical Framework

This study is governed by two overlapping ethical frameworks: the *National Statement on Ethical Conduct in Human Research* (NHMRC, 2023 update) and the *OMXUS Principles* — the non-negotiable ethical architecture of the system being tested. Where these frameworks reinforce each other, we note the alignment. Where they create additional obligations beyond the National Statement, we adopt the more stringent standard.

2.1 National Statement Compliance

This study satisfies the four values of the National Statement:

1. **Research Merit and Integrity:** The evidence synthesis (companion paper) establishes that the research question is meaningful, the methodology is appropriate, and the pilot is the minimum viable study to resolve empirical unknowns that cannot be addressed by modelling alone (Section 3).

2. **Justice:** The benefits and burdens of the research are fairly distributed. Participants are drawn from the community that would benefit from the system. No population is excluded without safety justification. No population bears disproportionate risk (Section 6.6).

3. **Beneficence:** The expected benefit (faster emergency response, improved community cohesion) is proportionate to the identified risks, all of which are mitigated (Section 5).

4. **Respect for Persons:** Participation is voluntary, informed consent is comprehensive, withdrawal is unconditional, and data sovereignty is maintained (Sections 6.1, 6.7).

2.2 OMXUS Principles Alignment

The OMXUS system is built on six hierarchically ordered principles. Three are absolute constraints (cannot be traded off); three are implementation requirements. The pilot study must satisfy all six.

2.2.1 Principle 1: Cannot Affect Individual Freedom (Absolute)

Collective decisions govern collective resources. No vote can constrain what you do with your own body, time, relationships, or property.

Application to this study:

- Responding to an alert is *always* voluntary. No social, reputational, or system-level penalty exists for non-response. This is not merely a design choice — it is an architectural constraint. The system records no per-person response/non-response data visible to others.

- Participants may wear the ring or not, respond or not, withdraw or not. No behaviour is coerced, incentivised, or tracked at the individual level.

- The system cannot be used to mandate beliefs, associations, or actions. It is a tool that enables voluntary mutual aid.

2.2.2 Principle 2: Non-Maleficence — Architectural, Not Promissory (Absolute)

The system cannot be weaponised against its users. Not "we promise not to" — architecturally impossible.

Application to this study:

- **Identity protection:** Alert broadcasts contain no personal identifier. Responders learn "an emergency exists nearby" — not who triggered it. This is enforced by the cryptographic protocol (Appendix C), not by policy.

- **Location protection:** Location is shared only during an active alert, only to devices within mesh range, and only for the alert duration. 15-minute session key rotation prevents temporal linkability. There is no continuous location tracking — the architecture does not support it.

- **No targeting mechanism:** The system has no mechanism for targeting individuals for punishment, surveillance, or social sanction. This is architectural: the data structures and protocols do not contain the fields that would be required.
- **No central data access:** Alert data is end-to-end encrypted. The research team accesses only de-identified, aggregated telemetry. Individual alert content is not accessible to researchers, OMXUS, or any third party.

2.2.3 Principle 3: Justice = Prevention Only (Absolute)

The system's model of justice is prevention, not punishment. Retribution is meaningless; only prevention matters.

Application to this study:

- The system is designed to prevent harm by reducing response times (the "empty minutes" problem), not to identify or punish perpetrators after the fact.
- If misuse occurs during the pilot (false alarms, harassment), the response is education, support, or exclusion from the study — not punishment, public shaming, or referral for sanction.
- Alert data will *not* be provided to law enforcement for investigative purposes except where required by mandatory reporting obligations (Section 6.4) or where a participant voluntarily provides their own data. The system is not a surveillance tool.

2.2.4 Principle 4: Transparent Accountability (Implementation)

Everyone sees the same thing. No hidden watchers. No asymmetric knowledge.

Application to this study:

- All study protocols, data collection instruments, and analysis plans are public (pre-registered, open data).
- Participants are told exactly what data is collected, by whom, for what purpose, and how long it is retained. There is no hidden data collection.
- The DSMB has full access to all study data. The PI has no information advantage over the DSMB.
- Findings — positive, negative, or ambiguous — will be published openly.

2.2.5 Principle 5: Telemetry for Humans (Implementation)

Your data works FOR you. This is not surveillance OF you — it is intelligence ABOUT you, owned BY you, serving YOU.

Application to this study:

- Participants own their data. They can request export or deletion at any time.
- Data collected during the study serves participants (faster emergency response) and the community (evidence for better systems), not commercial interests.
- No participant data will be sold, licensed, or shared with third parties for commercial purposes.
- The distinction between surveillance (hidden collection, asymmetric power, used against you) and telemetry (transparent, owned by you, serves your interests) is maintained throughout the study design.

2.2.6 Principle 6: Zero Effort, Enjoyable, Instant Rewards (Implementation)

Every interaction must provide immediate value.

Application to this study:

- The NFC ring is designed for zero-friction activation (gross motor triple-tap), specifically because the people who most need to trigger an alert are under acute stress with degraded fine motor control.
- Participation burden is minimised: 30-minute onboarding, 3 short surveys, no ongoing obligations.
- The system provides immediate feedback ("2 people are coming, ETA <2 min") because uncertainty during emergencies is itself harmful.

3 Background and Justification

3.1 The Response Time Gap

Emergency medicine literature documents a well-established relationship between response time and survival for time-critical conditions. Cardiac arrest survival drops approximately 10% per minute without CPR (AHA, 2020). Australian ambulance median response times are 7–14 minutes in urban areas and 20–45 minutes in rural settings.

Existing community first responder programs (GoodSAM, PulsePoint) have demonstrated that smartphone-alerted bystanders can arrive before professional responders, with measurable improvements in survival (Smith et al., 2020; MJA, 2025). However, these systems are limited to cardiac arrest, require smartphone interaction under stress, and depend on cellular connectivity.

3.2 What This Study Adds

This study tests a system that:

1. Covers *all* emergency types (medical, safety, welfare), not only cardiac arrest
2. Uses a wearable interface (NFC ring) requiring only gross motor activation
3. Propagates alerts via mesh networking (BLE, Wi-Fi Direct) without cellular dependency
4. Operates as a general community network, not limited to trained volunteers

Full evidence synthesis is provided in the companion paper: "Civic Proximity Response: An Evidence Synthesis for Wearable-Initiated Community Emergency Networks" (OMXUS Research, 2026).

4 Study Design and Methods

4.1 Setting

One suburban community in [STATE], Australia. Site selection criteria:

- Population density 1,000–5,000 per km^2
- Defined geographic boundaries (natural or administrative)
- Existing community organisations willing to partner (e.g., community centre, local council)
- Historical EMS response data available from ambulance service
- Not currently participating in another community safety intervention

4.2 Participants

4.2.1 Inclusion Criteria

- Adults aged 18 years or older
- Resident or regularly present ($\geq$4 days/week) in the study area
- Owns or has regular access to a compatible smartphone (Android 10+ or iOS 15+)
- Able to provide informed consent in English (multilingual materials available on request)
- Willing to wear NFC ring and have app installed for study duration

4.2.2 Exclusion Criteria

- Currently subject to an Apprehended Violence Order (AVO) or similar protective order as the respondent (to prevent system misuse against protected persons)
- Cognitive impairment that prevents informed consent (assessed by research team)
- Participation in the study would pose a safety risk as assessed by the research team (e.g., active psychosis, known violent behaviour)

4.2.3 Sample Size

Target: $n = 500$ participants.

Justification: At 500 participants over approximately 4 km^2, the network achieves a raw density of 125/km^2. With an estimated willingness factor of $w = 0.20$, effective responder density is 25/km^2, yielding an expected nearest-responder distance of $\sim$100m and estimated response time of 1–3 minutes. Based on Australian emergency incidence data ($\sim$1 per 4,600 people per day), the pilot expects 40–100 alert events over 12 months — sufficient for descriptive statistics on response times and acceptance rates.

4.2.4 Recruitment

Recruitment via:

1. Community partner organisations (letterbox drop, community centre posters)
2. Local council communication channels
3. Word-of-mouth from enrolled participants (snowball)
4. Local media coverage (newspaper, community radio)

No financial incentive for participation. Participants receive the NFC ring and app at no cost and may keep the ring after the study.

4.3 Intervention

4.3.1 Hardware

Each participant receives:

- One NFC ring (passive, no battery, waterproof, multiple sizes available)
- Smartphone app installed on their device (Android / iOS)

4.3.2 Training

All participants complete a 30-minute onboarding session covering:

1. How to activate an alert (triple tap on ring, or in-app button)
2. How to cancel a false activation
3. What to do when receiving an alert (acknowledge, move toward if safe, call 000 if needed)
4. Explicit instruction: **always call 000 for serious emergencies**
5. Explicit instruction: **never enter a dangerous situation**
6. Explicit instruction: **you are never required to respond — non-response has no consequence**
7. What to do if you encounter a deceased person (do not touch, call 000, stay if safe, wait for research debrief)
8. What to do in a mental health crisis (be present, do not restrain, call 000 and/or mental health crisis line)
9. How to withdraw from the study
10. Privacy: what data is collected, how it is stored, how to request deletion
11. Mandatory reporting obligations that apply during the study (Section 6.4)

Onboarding includes basic first aid guidance (recovery position, CPR awareness, direct pressure for bleeding) delivered via the app. This does not constitute formal first aid certification.

4.3.3 System Operation

When a participant activates an alert:

1. Ring transmits BLE signal to paired smartphone
2. Smartphone constructs alert packet (timestamp, coarse location, emergency type if specified)
3. Alert propagates via BLE and Wi-Fi Direct to nearby participants' devices
4. Nearby participants receive audio/haptic notification with coarse distance and direction
5. Responders acknowledge ("going", "calling 000", or "observing")
6. Acknowledgments visible to alerter ("2 people are coming, ETA <2 min")
7. Alert automatically expires after 30 minutes or manual resolution

The system operates alongside existing emergency services at all times.

4.4 Outcomes

4.4.1 Primary Outcome

Median time from alert activation to first physical contact by a community responder (minutes), compared with historical median EMS response time for the same geographic area.

4.4.2 Secondary Outcomes

1. Alert acceptance rate (proportion of nearby participants who acknowledge and respond)
2. Alert acceptance rate by emergency type, time of day, and responder demographics
3. False alarm rate (proportion of activations that are non-emergency)
4. Change in acceptance rate over time (false alarm fatigue measure)
5. Mesh network alert propagation latency (seconds)
6. NFC ring activation rate versus in-app activation rate
7. Responder adverse events (injury or psychological distress during response)
8. Participant-reported changes in perceived safety (validated survey, pre/post)
9. Participant-reported social cohesion (adapted Sampson Collective Efficacy scale, pre/post)

4.5 Data Collection

Table 2: Data collection instruments and schedule.

Instrument	Baseline	6 months	12 months
Demographics survey	✓		
Perceived safety scale	✓	✓	✓
Collective efficacy scale	✓	✓	✓
First aid confidence scale	✓		
System usability scale		✓	✓
App event logs (automated)		Continuous	
Post-incident debrief		Within 48h of each alert event	
Focus groups (subset)			✓

4.6 Statistical Analysis

4.6.1 Pre-registration

The analysis plan will be pre-registered with the Australian New Zealand Clinical Trials Registry (ANZCTR) prior to first participant enrolment.

4.6.2 Primary Analysis

Comparison of median community responder contact time with historical EMS median response time using the Mann–Whitney U test (non-parametric, appropriate for skewed time distributions).

4.6.3 Secondary Analyses

- Acceptance rate modelling: logistic regression with emergency type, time, distance, and cumulative false alarm exposure as predictors
- Fatigue analysis: time-series analysis of acceptance rate with false alarm exposure as covariate

- Pre/post survey comparisons: paired t-tests or Wilcoxon signed-rank tests as appropriate
- Qualitative analysis of focus groups: thematic analysis (Braun & Clarke, 2006)

5 Risk Assessment

5.1 Identified Risks and Mitigations

Risk	Likelihood	Severity	Mitigation
Responder injury during response	Low	High	Training explicitly prohibits entering dangerous situations. "Observe and report" is a valid response. Responders are never dispatched — they choose whether to respond. Insurance/indemnity provisions. Responder safety protocol (Appendix E).
False alarm causing alarm fatigue or distress	Moderate	Low	Rate limiting (max 3 alerts/day per person). Confirmation gesture required. False alarm feedback mechanism. Automatic suppression of repeated false triggers.
System misuse for stalking or harassment	Low	High	No continuous location tracking. Location shared only during active alert. 15-minute key rotation prevents tracking. Alerts contain no personal identifier. Participants on AVOs excluded. Abuse reports trigger immediate investigation. See Appendix C.
Participant relies on system instead of calling 000	Low	High	Training repeatedly emphasises 000 as primary. App displays "Call 000" prompt on every alert screen. System explicitly positioned as supplementary. Consent form states this clearly.
DV perpetrator uses system to locate victim	Low	High	Silent activation mode. No identity in broadcast. Location only visible to responders within mesh range (not globally). AVO holders excluded. DV-specific protocol (Appendix F).
Responder psychological distress after traumatic incident	Moderate	Moderate	Post-incident debrief within 48h. Referral to support services. Opt-out mechanism at any time. Responder wellbeing protocol (Appendix E). Research team includes psychologist.

Risk	Likelihood	Severity	Mitigation
Responder encounters deceased person	Low	High	Training includes protocol (do not touch, call 000, remain if safe, research debrief mandatory within 24h). Critical incident support activated automatically. Appendix E.
Mental health crisis escalation	Low–Mod	Moderate	Training: be present, do not restrain, call 000 or crisis line. App includes mental health crisis numbers. Debrief covers both alerter and responder wellbeing.
Data breach of alert logs	Low	Moderate	All alert data encrypted at rest (XChaCha20-Poly1305). Minimal data collection. Logs auto-delete after 90 days. De-identification before analysis. Full architecture in Appendix G.
System failure during genuine emergency	Moderate	Moderate	System is supplementary — 000 remains available. Participants trained in 000 as primary. System failure logged.
Community conflict over non-response	Low	Low	No penalty for non-response (architectural — Principle 1). Training establishes voluntary culture. Acknowledgment system is anonymised.
Social pressure to respond creating obligation	Low–Mod	Moderate	Anonymised acknowledgments ("2 people responding", not names). No individual response records visible to others. No gamification of response. No leaderboards. Voluntary nature reinforced in every communication.
Interaction with police at scene	Moderate	Moderate	Responders trained: identify yourself as a community responder, cooperate with police, do not interfere with police operations, do not provide alert data to police (refer to research team). Police liaison protocol (Appendix D).
Children present at emergency scene	Low–Mod	High	Responders trained to prioritise child safety. Mandatory reporting obligations apply (Section 6.4). Children cannot be study participants but may be beneficiaries.

5.2 Overall Risk Assessment

The overall risk to participants is assessed as **low–moderate**. The primary risk (responder injury) is mitigated by the voluntary nature of response and explicit training against entering dangerous situations. The system adds a supplementary layer to existing emergency infrastructure; it does not replace or interfere with existing services.

The OMXUS architectural principles (Section 2.2) provide additional protection beyond standard research safeguards: non-maleficence is enforced by cryptographic protocol, not by policy promise; individual freedom is preserved by the absence of coercive mechanisms, not by rules against their use.

5.3 Insurance and Indemnity

[TO BE COMPLETED — institutional indemnity / professional indemnity / participant insurance details]

5.4 Good Samaritan Protections

All Australian states and territories have Good Samaritan legislation providing civil liability protection for persons who assist others in emergencies in good faith and without expectation of reward. Participants will be informed of the relevant legislation for their jurisdiction during onboarding.

Key provisions (vary by state):

- **NSW:** Civil Liability Act 2002, s 57
- **VIC:** Wrongs Act 1958, s 31B
- **QLD:** Law Reform Act 1995, s 16
- **SA:** Civil Liability Act 1936, s 74
- **WA:** Civil Liability Act 2002, s 5AB

6 Ethical Considerations

6.1 Informed Consent

Written informed consent obtained from all participants prior to enrolment. The Participant Information Sheet and Consent Form (PICF) are appended (Appendix A).

Consent covers:

1. Nature and purpose of the study
2. What participation involves (wearing ring, having app installed, potentially responding to alerts)
3. Voluntary nature of both participation and response to alerts
4. Right to withdraw at any time without consequence
5. Data collection, storage, and deletion procedures
6. Known risks and mitigations
7. Mandatory reporting obligations (Section 6.4)
8. That alert data will not be provided to law enforcement except as required by law
9. Contact details for research team, HREC, and independent complaints process

6.2 Voluntary Response

It is critical that participants understand:

> **You are never required to respond to an alert.** Receiving an alert does not create any obligation, legal or social, to take any action. You may ignore any alert for any reason. There is no penalty, consequence, or record of non-response.

This statement appears in: the consent form, the onboarding session, the app welcome screen, and every alert notification.

Protection against social pressure: The system is designed to prevent informal social pressure to respond:

- Acknowledgments are anonymised ("2 people responding", not names)
- No individual response history is visible to other participants
- No gamification, leaderboards, or response counts
- Non-response is not logged in any participant-visible record
- The system architecturally cannot distinguish between "chose not to respond" and "was not near phone" — both look identical

6.3 Privacy and Data Protection

6.3.1 Data Minimisation

- No continuous location tracking
- Alert broadcasts contain no personal identifier
- Location shared only during active alert, only to nearby devices
- Session keys rotate every 15 minutes (preventing temporal linkability)
- Relay nodes cannot read alert content (relay blindness — see Appendix C)

6.3.2 Data Sovereignty

Consistent with OMXUS Principle 5 (Telemetry for Humans):

- Participants own their data at all times
- Participants can request a full export of their data in machine-readable format
- Participants can request deletion of their data at any time (within 14 days)
- No participant data will be sold, licensed, or shared with third parties for commercial purposes
- Data collected during the study is used for research purposes only, as specified in the consent form
- After study completion, de-identified aggregated data is published; individual-level data is destroyed

6.3.3 Storage and Retention

- Alert event logs: encrypted at rest (XChaCha20-Poly1305), auto-deleted after 90 days (or earlier on participant request)
- Survey data: de-identified at point of collection, stored on encrypted institutional servers
- Mesh network telemetry: aggregated only, no individual-level data retained
- Participant identifiers: stored separately from research data (linked by study ID only)
- Full data flow architecture: Appendix G

6.3.4 Compliance

The study complies with:

- Australian Privacy Act 1988
- Australian Privacy Principles (APPs)
- National Statement on Ethical Conduct in Human Research (NHMRC, 2023 update)
- Institutional data governance requirements
- OMXUS data principles (Principle 5: data works for the participant, not against them)

6.4 Mandatory Reporting Obligations

Researchers and participants may encounter situations during the study that trigger mandatory reporting obligations under Australian law. These obligations override data protection commitments and are disclosed to participants during consent.

6.4.1 Situations Requiring Mandatory Reporting

Situation	Legal Obligation	Study Protocol
Child abuse or neglect observed by researcher	Mandatory reporting under state/territory child protection legislation	Research team member reports to relevant child protection authority immediately. Event recorded as SAE.
Child abuse or neglect disclosed during debrief	Mandatory reporting	Researcher explains obligation to participant, reports to authority. Participant supported.
Imminent risk of serious harm to self or others	Duty of care / common law	Call 000. Research team notified immediately. DSMB informed within 24h.
Terrorism-related information	Criminal Code Act 1995, Division 102	Report to Australian Federal Police.

Situation	Legal Obligation	Study Protocol
Discovery of a deceased person during response	Coroner's Act (state/territory)	Do not touch. Call 000. Remain at scene if safe. Critical incident support for responder within 24h.

6.4.2 Participant Notification

Participants are informed during consent that:

1. The research team has mandatory reporting obligations that override confidentiality in specific circumstances (listed above)
2. If a participant discloses information during a debrief that triggers a mandatory report, the researcher will explain the obligation before making the report
3. Mandatory reports are made to the relevant authority, not to OMXUS, other participants, or law enforcement (unless law enforcement *is* the relevant authority for that category)

6.5 Law Enforcement Interaction

6.5.1 Alert Data and Police

Study alert data will *not* be voluntarily provided to law enforcement for investigative purposes. This position is based on:

- OMXUS Principle 3 (justice = prevention, not investigation/punishment)
- The system's purpose is emergency response, not evidence gathering
- Providing data to police would undermine participant trust and willingness to use the system, directly harming its effectiveness
- The cryptographic architecture means minimal useful data exists in any case (no identity in alerts, auto-deletion, relay blindness)

Exception: If a valid court order or warrant requires disclosure, the research team will comply with the law. Participants are informed of this possibility in the consent form.

6.5.2 Responder-Police Interaction at Scene

Participants who respond to an alert may encounter police at the scene. Training covers:

1. Identify yourself as "a community member responding to a notification" — not as an OMXUS representative or study participant (to avoid unnecessary complications)
2. Cooperate with police instructions
3. Do not provide your phone or device to police without a warrant
4. Do not answer questions about the alert system or other participants — refer to the research team
5. Contact the research team if police request study-related information

6.6 Vulnerable Populations

6.6.1 Domestic and Family Violence Survivors

- Silent activation mode (no audible alert on activating device)
- DV support service information integrated into onboarding (1800RESPECT, state DV lines)
- AVO respondents excluded from participation
- Research team includes DV-informed member
- Participants can request exclusion from receiving alerts from specific individuals (if known to them)
- Full DV safety protocol: Appendix F

6.6.2 Children and Minors

Children are *not* study participants (minimum age 18). However, children may be:

- Present at emergency scenes that participants respond to
- Beneficiaries of the system (a parent participant can trigger an alert for a child's emergency)
- Household members of participants

Safeguards:

- Responder training includes child-specific scenarios (lost child, injured child, child in distress)
- Mandatory reporting obligations apply if child abuse or neglect is observed (Section 6.4)
- Responders are trained: do not take a child away from a scene; call 000; stay and be a visible adult presence
- No data about children is collected by the study

6.6.3 Aboriginal and Torres Strait Islander Peoples

- Community consultation prior to site selection if study area includes significant Indigenous population
- Culturally appropriate onboarding materials developed in consultation with Indigenous advisors
- AIATSIS Code of Ethics for Research with Aboriginal and Torres Strait Islander Peoples observed
- Local Indigenous advisory input sought where appropriate
- Acknowledgment that Western emergency response models may not align with Indigenous community structures; flexibility in implementation

6.6.4 People with Disability

- Ring available in multiple sizes and form factors (ring, bracelet, card)
- App designed to WCAG 2.1 AA accessibility standards
- Alternative activation methods for participants with motor impairment
- Assistance available for onboarding
- Participants with disability are not assumed to be only alerters; they may also be responders if they choose

6.6.5 People with Mental Health Conditions

- Active psychosis or conditions involving significant risk of harm to others is an exclusion criterion (assessed at enrolment by research team with clinical input)
- Participants with managed mental health conditions (anxiety, depression, PTSD) are not excluded but are offered additional support during onboarding
- If a participant's mental health deteriorates during the study (identified via debrief or self-report), the research team facilitates referral to appropriate services and discusses whether continued participation is appropriate
- Responders who encounter a mental health crisis are trained to: be present, be calm, not restrain, call 000 or the mental health crisis line (13 11 14), and request post-incident debrief

6.6.6 Culturally and Linguistically Diverse (CALD) Communities

- Onboarding materials available in community languages spoken in the study area (identified during site selection)
- Interpreter services available for onboarding sessions
- Awareness that emergency response norms vary across cultures (e.g., attitudes to bystander intervention, comfort with strangers approaching)
- Cultural liaison consulted during community engagement phase

6.7 Withdrawal

Participants may withdraw at any time by:

1. Contacting the research team (phone, email, or in-person)
2. Using the in-app withdrawal function
3. Simply ceasing to wear the ring and uninstalling the app

Upon withdrawal:

- All identifiable data deleted within 14 days
- Aggregated, de-identified data already incorporated into analyses is retained (as per consent)
- Ring may be returned or kept
- No questions asked, no pressure to continue, no cooling-off period requirements

6.8 Reporting of Adverse Events

- All adverse events (injury, psychological distress, system misuse) reported to PI within 24 hours
- Serious adverse events (hospitalisation, death, criminal conduct) reported to HREC within 72 hours
- DSMB reviews all adverse events quarterly and has authority to pause or terminate the study
- Critical incidents (death, serious injury, child safety concerns) trigger immediate DSMB meeting (within 48 hours)
- Annual progress report submitted to HREC

6.9 Commercialisation Ethics

The OMXUS project has a commercial dimension: the technology being tested may ultimately become a product. This creates ethical obligations beyond standard academic research:

1. **No commercialisation during study:** No data from this pilot will be used for marketing, investment solicitation, or commercial purposes until final results are published and peer-reviewed.
2. **Community benefit:** If the system is commercialised after the pilot, the study community will receive continued access to the system at no cost for a minimum of 24 months post-study. This is a written commitment, not a verbal assurance.
3. **Data firewall:** Pilot data is held by the research institution, not by OMXUS. OMXUS receives only the published results (same as any member of the public).
4. **Participant notification:** If the commercial plans for OMXUS change materially during the study (e.g., acquisition, pivot, cessation), participants will be notified.

6.10 Power Dynamics and Social Pressure

6.10.1 Researcher-Participant Power

The research team is also the technology developer. This creates a power dynamic where participants may feel pressure to report positive experiences or continue participation to "help the project." Mitigation:

- Surveys are anonymous
- Post-incident debriefs are conducted by a researcher who did not develop the technology
- Withdrawal is unconditional and requires no justification
- Participants are explicitly told during onboarding: "We need honest data. If the system doesn't work, we need to know. Negative feedback is as valuable as positive feedback."

6.10.2 Intra-Community Power

The system creates the possibility of informal social dynamics:

- "Good responder" social status (mitigated by anonymised acknowledgments)
- Pressure to participate from neighbours or community leaders (mitigated by clear voluntary messaging in all recruitment materials)
- Knowledge asymmetry between participants and non-participants (mitigated by community-wide information sessions, not just for enrolled participants)

7 Data Safety Monitoring Board

An independent DSMB will be established comprising:

1. An emergency medicine clinician not involved in the study
2. A biostatistician not involved in the study
3. A community representative from the study area
4. A privacy/data governance specialist
5. A psychologist with expertise in trauma and crisis intervention

Independence: No DSMB member may have any current or prior financial, employment, consulting, or advisory relationship with OMXUS. DSMB members will sign a conflict-of-interest declaration prior to appointment.

The DSMB will:

- Meet quarterly (or more frequently if triggered by adverse events)
- Review all adverse events and near-misses
- Review false alarm rates and fatigue indicators
- Review responder wellbeing indicators
- Have authority to pause enrolment, modify protocols, or terminate the study
- Provide written recommendations to the PI and HREC
- Conduct an emergency meeting within 48 hours of any critical incident

7.1 Stopping Rules

The study will be paused for DSMB review if:

- Any serious adverse event (hospitalisation or death) plausibly related to study participation
- Responder injury rate exceeds 1 per 100 response events
- False alarm rate exceeds 50% of total activations (sustained over 30 days)
- Participant withdrawal rate exceeds 30% (indicating community rejection)
- Any evidence of systematic misuse (stalking, harassment, coordinated false alarms)
- Any mandatory report to child protection services arising from study activities
- Any participant reports feeling coerced to respond or participate

8 Timeline

Table 5: Study timeline.

Phase	Duration	Activities
Ethics and approvals	Months 1–3	HREC submission, site agreements, ANZCTR registration
Community engagement	Months 3–4	Community information sessions, partner agreements (Appendix
Site preparation	Months 4–6	Emergency services MOU, hardware procurement, app testing
Recruitment	Months 6–9	Participant recruitment and onboarding (rolling)
Active deployment	Months 9–21	12-month active monitoring period
Data analysis	Months 21–24	Statistical analysis, qualitative analysis
Reporting	Months 24–26	Final report, publications, community debrief

8.1 Budget Summary

Table 6: Estimated budget.

Item	Cost (AUD)
NFC rings (500 × $15 incl. sizing/shipping)	$7,500
App development and maintenance (12 months)	$25,000
Mesh network hardware (LoRa nodes, 10 units)	$3,000
Community engagement and recruitment materials	$8,000
Translation and interpreter services	$5,000
Research assistant (0.5 FTE, 26 months)	$65,000
Clinical psychologist (incident debriefs, 0.1 FTE)	$15,000
Statistical analysis (independent contractor)	$10,000
DSMB costs (honoraria, meetings)	$8,000
Insurance/indemnity	$5,000
Emergency services liaison	$3,000
Contingency (10%)	$15,450
Total	**$170,950**

A Participant Information Sheet and Consent Form

A.1 Participant Information Sheet

PARTICIPANT INFORMATION SHEET

Study Title: Civic Proximity Response Pilot Study
Ethics Approval Number: [TO BE ASSIGNED]
Principal Investigator: [NAME], [INSTITUTION]
Contact: [PHONE] / [EMAIL]

What is this study about?

We are testing a new way to help people in emergencies get help faster. You will receive a special ring and a phone app. If you or someone near you has an emergency, you can tap the ring to alert nearby participants. If someone near you taps their ring, you'll get a notification and can choose to go help.

This does **not** replace calling 000. You should always call 000 for serious emergencies. The ring is an additional way to get immediate help from people who are already nearby.

What will I need to do?

- Attend a 30-minute onboarding session
- Wear the NFC ring (or carry it)
- Have the study app installed on your phone
- Complete 3 short surveys (start, 6 months, 12 months)
- Optionally: respond to emergency alerts from nearby participants

Do I have to respond to alerts?

No. You never have to respond. Receiving an alert does not create any obligation. You can ignore any alert for any reason. There is no penalty, record, or consequence for not responding. The system does not track whether you respond or not.

What are the risks?

- If you choose to respond to an alert, you may encounter an upsetting situation (including serious injury, death, or violence). You are trained to stay safe and never enter a dangerous situation.
- You may experience psychological distress after responding to a traumatic event. Free, confidential support is available through the study.
- You may receive false alarms, which can be annoying. The system limits these.
- Your approximate location is shared with nearby participants only during an active alert you trigger. There is no tracking at other times.

What are the benefits?

- You may receive faster help in an emergency from people near you
- You contribute to research that could improve emergency response for everyone
- You keep the NFC ring after the study

How is my privacy protected?

- No continuous location tracking — ever
- Location only shared during an active alert you trigger, only to nearby devices
- All data encrypted using military-grade encryption
- Alert logs automatically deleted after 90 days
- Research data is de-identified — your name is never attached to results
- You can request deletion of your data at any time
- Your data will not be given to police, employers, insurers, or anyone else (except where required by law — see below)

Will my data be given to police?

No. The research team will not voluntarily provide your data to police or other law enforcement. The only exception is if a court issues a legal order requiring disclosure, which we would inform you about. Alert data does not contain your name or identity in any case.

Are there mandatory reporting obligations?

Yes. If a researcher observes or is told about child abuse or neglect, or an imminent risk of serious harm to someone, they are required by law to report this to the relevant authority. The researcher will tell you about this obligation if it arises. This is the only circumstance where confidentiality may be limited.

Can I withdraw?

Yes. You can withdraw at any time by contacting the research team, using the app, or simply stopping participation. Your data will be deleted within 14 days. There is no penalty for withdrawal. You do not need to give a reason.

What support is available?

- Free, confidential post-incident psychological support through the study
- 1800RESPECT (1800 737 732) — family and domestic violence support
- Lifeline (13 11 14) — crisis support
- Beyond Blue (1300 22 46 36) — mental health support

Who do I contact?

- Research team: [NAME], [PHONE], [EMAIL]
- Ethics committee: [HREC NAME], [PHONE], [EMAIL]
- Independent complaints: [INSTITUTION COMPLAINTS OFFICER], [PHONE]

A.2 Consent Form

CONSENT FORM

Study Title: Civic Proximity Response Pilot Study
Ethics Approval Number: [TO BE ASSIGNED]

I have read and understood the Participant Information Sheet (Version 3.0, February 2026).

[ ] I understand the purpose and procedures of this study.

[ ] I understand that my participation is voluntary and I can withdraw at any time without penalty.

[ ] I understand that responding to emergency alerts is **voluntary** and I am never required to respond.

[ ] I understand that this system **does not replace Triple Zero (000)** and I should always call 000 for serious emergencies.

[ ] I understand the risks described in the information sheet, including the possibility of encountering distressing situations (including serious injury or death) if I choose to respond to alerts.

[ ] I understand that **I should never enter a dangerous situation** when responding to an alert.

[ ] I understand how my data will be collected, stored, and protected as described in the information sheet.

[ ] I understand that my data will not be provided to police or law enforcement except under court order.

[ ] I understand the mandatory reporting obligations described in the information sheet.

[ ] I consent to the research team accessing de-identified alert event data from my participation.

[ ] I have had the opportunity to ask questions and have had them answered satisfactorily.

[ ] I consent to participate in this study.

Participant Name: _____ **Date:** _____

Participant Signature: _____

Researcher Name: _____ **Date:** _____

Researcher Signature: _____

A signed copy of this form will be given to you. The original will be retained by the research team.

B Survey Instruments

B.1 Perceived Safety Scale (Adapted)

Participants rate agreement (1 = Strongly Disagree to 5 = Strongly Agree):

1. I feel safe walking in my neighbourhood during the day.
2. I feel safe walking in my neighbourhood at night.
3. If I had an emergency, someone nearby would help me.
4. I would feel comfortable asking a neighbour for help.
5. I trust the people in my neighbourhood.
6. I would intervene if I saw someone in my neighbourhood who needed help.
7. I believe my neighbourhood is becoming safer / staying the same / becoming less safe.

B.2 Collective Efficacy Scale (Adapted from Sampson et al., 1997)

Social cohesion subscale:

1. People around here are willing to help their neighbours.
2. This is a close-knit neighbourhood.
3. People in this neighbourhood can be trusted.
4. People in this neighbourhood generally don't get along with each other. (R)
5. People in this neighbourhood share the same values.

Informal social control subscale ("How likely is it that your neighbours would intervene if. . . "):

1. Children were showing disrespect to an adult.
2. A fight broke out in front of their house.
3. Someone was being assaulted.
4. Someone appeared to be having a medical emergency.
5. A neighbour's property was being vandalised.

B.3 Post-Incident Debrief Guide

Conducted within 48 hours of any alert event. Semi-structured interview:

1. What happened? (Participant's account)
2. How did you activate the alert / receive the alert?
3. How long did it take for someone to arrive? (Participant's estimate)
4. Did you also call 000? If yes, which arrived first?
5. How did you feel during the event?

6. How do you feel now?
7. **Wellbeing check:** Are you experiencing any of the following: intrusive thoughts, difficulty sleeping, heightened anxiety, avoidance of the area? (Screen for acute stress reaction)
8. Is there anything about the system you would change?
9. Do you need any support? (Referral to services if indicated)
10. **If deceased person encountered:** Additional questions administered by clinical psychologist, not research assistant. Mandatory referral to support services.

C Technology Safety Specification

This appendix describes the cryptographic and architectural safeguards that enforce OMXUS Principle 2 (Non-Maleficence) at the protocol level. These guarantees are *architectural*, not policy-based: the system cannot be reconfigured to violate them without replacing the core protocol.

C.1 Cryptographic Primitives

Table 7: Cryptographic primitives used in the ring SOS protocol.

Function	**Algorithm**	**Purpose**
Identity key (IK)	Ed25519	Long-lived device identity
Derived key (DK)	HKDF-SHA256	Epoch-specific key derivation
Session key (SK)	Rotated every 15 min	Prevents temporal linkability
Alert encryption	XChaCha20-Poly1305	Authenticated encryption of alert content
Message encoding	CBOR (RFC 8949)	Compact binary serialisation

C.2 Privacy Guarantees

1. **No identity in broadcasts:** SOS alert messages (SOS_INIT, SOS_ACK) contain no personal identifier, name, phone number, or account reference. The only content is: timestamp, coarse location (grid cell, not GPS), emergency category, and cryptographic session token.
2. **Session key rotation:** Session keys rotate every 15 minutes (epoch boundary). An observer monitoring broadcasts cannot link two alerts from the same device across epoch boundaries. This prevents:
   - Movement tracking by broadcast observation
   - Building activity profiles from alert patterns
   - Correlating a person's location across time periods
3. **Relay blindness:** Community relay nodes (devices that forward alerts beyond direct BLE range) process encrypted payloads they cannot decrypt. A relay learns only: "an alert exists in my area" and "I should forward it." It cannot determine: the alerter's identity, precise location, emergency type, or whether the alert is genuine.
4. **Rate limiting:**
   - 3 SOS alerts per 24 hours per identity (prevents spam/misuse)

- 6 audible notifications per hour per helper device (prevents alarm fatigue)
- Flood protection: if >20 SOS in 5 minutes in a mesh bucket, switch to degraded mode (silent forwarding, no audible alerts)

5. **Escalation thresholds:** Alerts escalate to wider relay network only if <2 acknowledgments within 45 seconds. Most alerts are resolved within the immediate BLE neighbourhood (∼100m) without any relay involvement.

C.3 Threat Model

The protocol is designed to be secure against the following adversaries:

Table 8: Threat model for the ring SOS protocol.

Adversary	Capability	Protection
Passive observer	Monitors BLE broadcasts	No identity in broadcasts; session key rotation
Malicious relay	Forwards/drops/modifies alerts	End-to-end encryption; relay cannot read content
Stalker	Attempts to track specific person	15-min key rotation; no linkability across epochs
DV perpetrator	Attempts to locate victim	No identity; coarse location only; silent mode
Law enforcement	Requests alert data	Minimal data exists; auto-deletion; no central store
Research team	Has access to study infrastructure	Receives only de-identified aggregates; no access to individual alert content

C.4 What the Technology Cannot Prevent

Transparency requires acknowledging limitations:

- The system cannot prevent a participant from verbally disclosing that they triggered or responded to an alert
- If two participants are in the same room, one can observe the other's phone receiving an alert (mitigated by silent mode)
- A sophisticated adversary who controls many devices in an area could perform traffic analysis (mitigated by relay blindness and rate limiting, but not fully eliminated)
- The ring itself is a visible object; wearing it signals study participation

D Emergency Services Integration Protocol

D.1 Memorandum of Understanding

Prior to study commencement, a Memorandum of Understanding (MOU) will be sought with the relevant state/territory ambulance service and, if possible, the local police area command. The MOU will establish:

1. **Notification:** Emergency services are informed that a community response network is operating in the study area. They will encounter "community responders" at some emergency scenes.
2. **Supplementary positioning:** The system is supplementary to 000. It does not dispatch, does not prioritise, does not override, and does not communicate with the dispatch system. It is a separate layer.
3. **No interference:** Participants are trained to yield to professional responders immediately upon arrival and to follow professional instructions.
4. **Data sharing:** Historical (anonymised) EMS response time data for the study area will be requested for comparison purposes. No study data will be shared with emergency services.
5. **Incident reporting:** If an incident during the study involves EMS, the research team will coordinate with EMS for debriefing purposes (with participant consent).

D.2 Scene Protocol

When professional emergency services arrive at a scene where a community responder is present:

1. Community responder immediately identifies themselves: "I'm a neighbour / community member. I was nearby."
2. Community responder provides a brief handover: what they observed, what they did, current status of the person in need
3. Community responder steps back and follows professional instructions
4. Community responder does not leave the scene until released by emergency services or research team (for debrief purposes, if applicable)

D.3 Scenario: Police Investigation at Scene

If police at the scene wish to interview the community responder:

- Responder cooperates as any member of the public would (they have no special legal status)
- Responder does not disclose details about the alert system, other participants, or study operations — refers these questions to the research team
- Responder does not hand over their phone or device without a warrant
- Research team is contacted and available 24/7 during the study for police enquiries

E Responder Safety and Wellbeing Protocol

E.1 Before Response: Training

All participants receive training that emphasises:

1. **Your safety comes first.** If the situation appears dangerous, do not approach. Valid responses include: calling 000, observing from a safe distance, doing nothing.

2. **You are not a first responder.** You have no duty to provide medical care, restrain anyone, or take any action beyond being present and calling for professional help.
3. **"Observe and report" is a complete response.** Arriving near a scene, assessing it as unsafe or beyond your capability, calling 000, and waiting — this is a full, valid, valued response.

E.2 During Response: Safety Rules

1. Do not enter a building if you cannot see what is inside
2. Do not approach a violent or aggressive person
3. Do not attempt to restrain anyone
4. Do not move an injured person unless they are in immediate danger (fire, traffic)
5. Do not provide medical interventions beyond basic first aid (recovery position, CPR, direct pressure)
6. If you feel unsafe at any point, leave immediately

E.3 After Response: Wellbeing Support

E.3.1 Routine Debrief

Within 48 hours of any alert event, a research team member contacts both the alerter and all responders for a structured debrief (Appendix B, Post-Incident Debrief Guide).

E.3.2 Critical Incident Response

If the incident involved any of the following, a clinical psychologist (not a research assistant) conducts the debrief:

- Death or suspected death
- Serious injury with visible trauma
- Violence or assault
- Child in danger
- Responder reports feeling distressed, shaky, or "not okay"

Critical incident protocol:

1. Immediate: responder contacted within 4 hours (phone)
2. 24 hours: in-person or video debrief with clinical psychologist
3. 7 days: follow-up welfare check
4. 30 days: second follow-up
5. Ongoing: referral to external psychological services if needed (funded by study)

E.3.3 Opt-Out from Responder Role

At any time, a participant can disable the responder function in the app while retaining the ability to trigger alerts. This means they can still call for help but will not receive others' alerts. This can be done:

- Temporarily (e.g., "I need a break after that incident")
- Permanently (for the remainder of the study)
- Without explanation or approval

F Domestic and Family Violence Safety Protocol

This protocol addresses the specific risks and safeguards for participants who are experiencing or have experienced domestic and family violence (DFV).

F.1 Design Safeguards

1. **Silent activation:** The ring can be configured for silent alert activation. No sound, no vibration, no screen change on the alerter's device. The alert propagates silently to nearby devices.
2. **No identity disclosure:** Alerts contain no personal identifier. A perpetrator monitoring nearby Bluetooth traffic learns only "an alert exists" — not who triggered it.
3. **Coarse location only:** Location in alerts is grid-cell level (approximately 100m^2), not GPS coordinates. This is sufficient for a responder to move toward the alert but not sufficient to pinpoint an exact room or address.
4. **AVO exclusion:** Participants who are the respondent to an active AVO, DVO, or equivalent protective order are excluded from the study. This is assessed at enrolment via self-declaration and, where feasible, verified against publicly available court records.
5. **Selective blocking:** Participants can request that a specific other participant not receive their alerts. This is implemented at the app level (blocked device IDs do not receive the alert) and does not require disclosure of the reason.

F.2 Onboarding for DFV-Affected Participants

During onboarding, all participants receive:

- Information about 1800RESPECT (1800 737 732) and state/territory DFV services
- Explanation of silent activation mode and how to configure it
- A private, one-on-one opportunity to discuss any safety concerns with a DFV-informed research team member
- An explicit statement: "If you are experiencing domestic violence, this system may be helpful to you, but it may also pose risks. We encourage you to discuss your situation with a DFV service before deciding whether to participate."

F.3 Scenario Protocols

F.3.1 Scenario: Responder arrives at a DFV situation

1. Do not enter the premises
2. Call 000 immediately
3. Remain at a safe distance and observe
4. Do not confront or engage with any person who appears aggressive
5. When police arrive, provide a brief account and step back
6. Contact research team for debrief

F.3.2 Scenario: Participant discloses DFV during the study

1. Research team member provides 1800RESPECT number and local DFV service contacts
2. Research team does *not* intervene directly in the DFV situation (this is for trained DFV workers)
3. If children are at risk, mandatory reporting obligations apply (Section 6.4)
4. Participant is offered the option to adjust their study participation (e.g., disable responder role, receive safety planning support)

F.3.3 Scenario: Perpetrator attempts to use system to locate victim

1. The system architecture prevents this (no identity in alerts, no continuous tracking, 15-minute key rotation)
2. If a participant reports suspected misuse, the research team investigates immediately
3. If misuse is confirmed, the perpetrator's participation is terminated and DSMB is notified
4. The participant's data is reviewed for any compromise (though the architecture minimises what data exists)

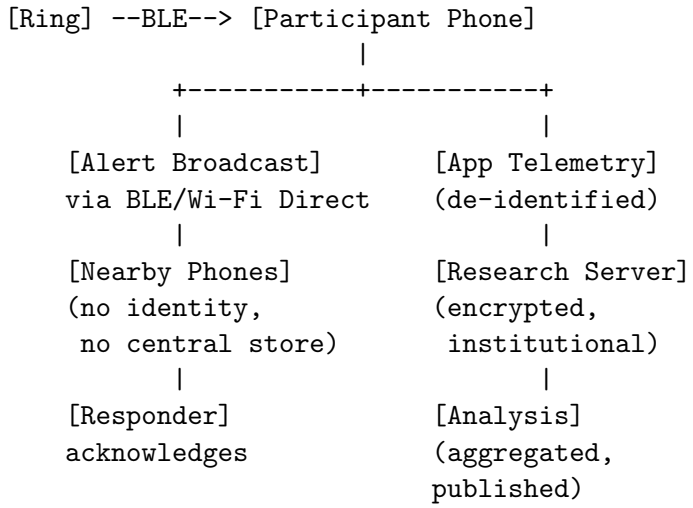
G Data Flow and Privacy Architecture

G.1 Data Categories

Table 9: Data categories, retention, and access.

Data Type	Collected By	Stored Where	Retention	Access
Alert event logs	App (automated)	Device only (encrypted)	90 days, then auto-deleted	Participant only
De-identified alert telemetry	App → research server	Institutional server (encrypted)	Study duration + 5 years	Research team, DSMB
Survey responses	Paper/online form	Institutional server	Study duration + 5 years	Research team
Participant identifiers	Consent form	Locked filing cabinet / encrypted file	Study duration + 5 years	PI and RA only
Mesh network metadata	App (automated)	Aggregated on server	Study duration	Research team
Post-incident debriefs	Research team (audio/notes)	Institutional server (encrypted)	Study duration + 5 years	Research team

G.2 Data Flow Diagram



G.3 Separation of Concerns

1. **Alert data never reaches OMXUS:** Alert broadcasts are device-to-device. They do not pass through any OMXUS server. OMXUS (the organisation) has no access to alert data.
2. **Research data is held by the institution:** De-identified telemetry and survey data are stored on institutional servers, not OMXUS infrastructure.
3. **Participant identifiers are separated:** The link between a participant's name and their study ID is held only in a locked file accessible to the PI and RA. It is not stored on any networked system.

4. **Published data is aggregated:** The open dataset published at study completion contains only aggregated, de-identified data. No individual participant's alert history, location history, or survey responses are published.

G.4 Participant Data Rights

Consistent with OMXUS Principle 5 and the Australian Privacy Principles:

1. **Right to access:** Participants can request a copy of all data held about them
2. **Right to correction:** Participants can request correction of inaccurate data
3. **Right to deletion:** Participants can request deletion of their data (within 14 days)
4. **Right to export:** Participants can request their data in a machine-readable format
5. **Right to know:** Participants are informed of any data breach affecting their data within 72 hours

H Community Engagement Plan

Community engagement is not merely a recruitment strategy. It is an ethical obligation: the study deploys a system *in* a community, and that community has the right to be informed, consulted, and heard — including those who choose not to participate.

H.1 Pre-Study Engagement (Months 3–4)

1. **Community information sessions:** At least 3 public sessions in the study area (community centre, library, school hall). Open to all residents, not just prospective participants. Sessions explain: what the study is, what the ring does, what data is collected, what risks exist, and how to raise concerns.
2. **Local council briefing:** Written briefing and in-person presentation to the local council or community board. Council endorsement is sought but not required; the study can proceed without it, but council opposition would trigger re-evaluation.
3. **Emergency services briefing:** State ambulance service and local police area command are briefed (see Appendix D).
4. **Community advisory group:** A group of 5–8 community members (mix of participants and non-participants) is established to provide ongoing input throughout the study. The group meets quarterly and has a direct channel to the DSMB.
5. **Aboriginal and Torres Strait Islander consultation:** If the study area includes significant Indigenous population, formal consultation with local Indigenous organisations or Elders is conducted before site confirmation. Indigenous advisors are invited to join the community advisory group.
6. **CALD community outreach:** Community leaders from culturally and linguistically diverse groups in the study area are contacted. Onboarding materials are translated. Interpreter services are arranged.

H.2 During Study (Months 6–21)

1. Community advisory group meets quarterly
2. Six-month community update: public session reporting on study progress (no individual data)
3. Mechanism for non-participants to raise concerns (email, phone, community advisory group)
4. Local media updates at PI's discretion (no individual data)

H.3 Post-Study (Months 24–26)

1. Community debrief session: public presentation of findings (positive, negative, and ambiguous)
2. Written summary in plain language distributed to all participants and community partners
3. Community advisory group consulted on dissemination approach
4. If system is continued post-study, community vote or consultation on whether to continue (consistent with OMXUS governance principles)

I References

1. AIATSIS. (2020). *Code of Ethics for Aboriginal and Torres Strait Islander Research*. AIATSIS, Canberra.
2. American Heart Association. (2020). Heart Disease and Stroke Statistics—2020 Update. *Circulation*, 141(9), e139–e596.
3. Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
4. Cohen, L.E. & Felson, M. (1979). Social Change and Crime Rate Trends. *American Sociological Review*, 44(4), 588–608.
5. Darley, J.M. & Latané, B. (1968). Bystander intervention in emergencies. *JPSP*, 8(4), 377–383.
6. Fischer, P., et al. (2011). The bystander-effect: A meta-analytic review. *Psychological Bulletin*, 137(4), 517–537.
7. MJA. (2025). Smartphone-activated volunteer responders and survival to discharge. *MJA*, 222(10).
8. NHMRC. (2023). *National Statement on Ethical Conduct in Human Research* (2023 update). Canberra.
9. OMXUS. (2026). Ring SOS Protocol Specification v0.1. Internal technical document.
10. OMXUS Research. (2026). Civic Proximity Response: An Evidence Synthesis. Internal paper.
11. Sampson, R.J., Raudenbush, S.W. & Earls, F. (1997). Neighborhoods and Violent Crime. *Science*, 277(5328), 918–924.

12. Smith, C.M., et al. (2020). Community First Responders in Real Emergencies. *Resuscitation*, 155, 152–159.