Alabama Rural Coalition for the Homeless, Inc.
Personable Identifiable Information Breach Policy

PII Policy Statement: ARCH's policy for managing a breach of PII in HMIS is rooted in its commitment to the highest standards of data security, confidentiality, and compliance with relevant regulations, including those set forth by the U.S. Department of Housing and Urban Development (HUD). The policy underscores ARCH's responsibility as the lead HMIS agency for the Alabama Balance of State to promptly and effectively address any breach of PII to protect the privacy and dignity of individuals accessing homeless services.

Procedures for Managing a Breach of PII:

1. **Detection and Assessment:** Upon discovery or notification of a potential breach of PII within the HMIS, ARCH promptly initiates an assessment. This assessment evaluates the scope, nature, and potential impact of the breach.

2. **Containment:** ARCH takes immediate steps to contain the breach, preventing any further unauthorized access or dissemination of PII.

3. **Notification:** If it is determined that the breach poses a risk of harm or compromise to individuals, ARCH follows a robust notification protocol. Affected individuals, partner agencies, and relevant authorities are notified in accordance with applicable regulations and best practices.

4. **Response Team Activation:** ARCH assembles a response team comprised of experts from various disciplines, including data security, legal, and communications. This team collaborates to orchestrate an effective response to the breach.

5. **Mitigation Measures:** ARCH implements mitigation measures to minimize the impact of the breach. These measures may include offering credit monitoring services to affected individuals, providing guidance on protective actions, and offering support to those impacted.

6. **Investigation:** A thorough investigation is conducted to ascertain the root cause of the breach. This investigation helps identify vulnerabilities and informs strategies to prevent future breaches.

7. **Documentation:** ARCH meticulously documents all aspects of the breach, including its discovery, response actions, and outcomes. This documentation is critical for regulatory compliance and future reference.

8. **Continuous Improvement:** Following the breach response, ARCH conducts a post-incident analysis to identify areas for improvement. Lessons learned are used to enhance security measures and refine breach response procedures.

9. **Communication:** Transparent and clear communication is maintained with affected individuals, partner agencies, regulatory bodies, and the broader community. ARCH remains committed to providing accurate information and updates throughout the breach management process.

10. **Training and Awareness:** ARCH continually invests in training and awareness programs to educate staff, partner agencies, and stakeholders about PII security best practices, thus fostering a culture of vigilance and accountability.

ARCH's policy and procedures for managing a breach of PII in HMIS reflect its unwavering commitment to data security, privacy, and compliance. These protocols ensure that any breach is addressed swiftly, transparently, and comprehensively, thereby upholding the trust of individuals seeking homeless services and the confidence of federal partners.

Adopted June 23, 2021