

MCCULLOUGH AGENCY

COMPREHENSIVE PRIVACY, SECURITY, & AI COMMUNICATIONS POLICY

AGENCY COMPLIANCE METADATA

Effective Date: October 15, 2026

Agency Representative: Doug McCullough, Privacy & Security Official

Legal Entity: McCullough Agency / Doug McCullough Insurance Agency LLC

Address: 2527 St. Clair River Dr., Algonac, MI 48001

Office/Text: (810) 209-4800 | Fax: (810) 963-1100

Website: www.mcculloughagency.com

1. PURPOSE, SCOPE, AND COMMITMENT TO PRIVACY

McCullough Agency ("Agency," "we," "our," or "us") respects the privacy and security of clients, prospective clients, associates, vendors, and website visitors. This document serves as the formal written policy regarding the protection, security, and lawful handling of information as required by federal and state laws.

- **Applicability:** This policy applies to all agency associates, temporary staff, contractors, vendors, and business partners. It covers oral, written, and electronic individually-identifiable health information (PHI), non-public personal financial information (NPI), and digital communication logs.
- **Regulatory Framework:** Our practices comply with applicable federal and Michigan requirements, including the Health Insurance Portability and Accountability Act (HIPAA) Title II, HITECH Act, Gramm-Leach-Bliley Act (GLBA), Telephone Consumer Protection Act (TCPA), A2P 10DLC requirements, and insurance privacy regulations.
- **Precedence:** In the event of conflicting regulations, the Agency will adhere to the most stringent requirement or consult legal counsel. These terms continue to apply even if the Agency ceases business operations.

2. DEFINITIONS

- **Access:** The ability or means to read, write, modify, or communicate data or use system resources.
- **Authentication:** The process of verifying the identity of an individual and their legal authority to access requested information.
- **Business Associate (BA) & Agreement (BAA):** A person/entity performing functions involving PHI on behalf of a Covered Entity, governed by a mandatory contract ensuring equivalent privacy protections.
- **Covered Entity:** Health plans, healthcare clearinghouses, or providers that transmit health information electronically.
- **De-identification:** The formal removal of key personal identifiers so remaining data cannot reasonably be re-identified or linked to an individual.

- **Minimum Necessary Standard:** The practice of limiting the use, disclosure, or request of PHI to the least amount necessary to accomplish the intended purpose.
- **Non-Public Personal Information (NPI):** Personally identifiable financial information provided by a consumer to obtain an insurance or financial product/service.
- **Protected Health Information (PHI):** Individually identifiable health information maintained or transmitted in any form (electronic, written, or oral) relating to past, present, or future physical/mental health conditions, provision of care, or payment.

3. INFORMATION WE COLLECT & SOURCES

We collect information reasonably necessary to provide insurance quotes, evaluate coverage, service policies, process payments, and ensure operational security.

Categories Collected

- **Identification & Contact:** Name, mailing address, phone numbers, email address, date of birth.
- **Insurance & Financial:** Policy details, coverage preferences, claim histories, premiums, bank account/routing numbers for premium processing.
- **Health Information:** Lawfully provided medical/dental information necessary for health, life, or disability underwriting and servicing.
- **Digital & AI Logs:** Message timestamps, opt-in/opt-out records, AI-assisted communication logs, IP addresses, and cookie data.

Sources of Data

Direct client submissions (forms, calls, texts), insurance carriers, third-party underwriting services, CRM platforms, and authorized service partners.

4. PERMITTED USES & DISCLOSURES OF INFORMATION

The Agency uses and discloses information for Treatment, Payment, and Health Care/Plan Operations (TPO) and administrative functions on behalf of covered entities:

- **Routine Operations:** Quoting, underwriting, policy issuance, enrollment, claim audits, commission processing, and customer service.
- **Required Disclosures:** Compliance reviews by the Secretary of HHS, law enforcement or judicial orders, workers' compensation compliance, and public health/oversight reporting.
- **Whistleblower Disclosures:** Associates may disclose PHI to health oversight agencies or retained legal counsel to report unlawful conduct or privacy violations.
- **Prohibited Uses & Sale:** We do not sell PHI or personal data. The sale of protected information requires express review and authorization by the Privacy Officer.

5. ARTIFICIAL INTELLIGENCE (AI) & AUTOMATED COMMUNICATIONS

We utilize AI systems, automated workflows, and customer management platforms to assist with general inquiries, appointment scheduling, and customer support.

- **Non-Binding Nature:** AI-generated messages are purely informational. AI tools cannot issue binding insurance quotes, modify policy terms, execute coverage determinations, or make final eligibility decisions. All binding actions require authorized human/carrier review.
- **Data Processing Controls:** Customer data sent to AI vendors is strictly limited to the minimum necessary for the immediate task. Vendor contracts must restrict data usage solely to approved agency services and prohibit data use for independent model training, third-party advertising, or profiling.
- **Human Oversight & Escalation:** Complex coverage evaluations, claims disputes, and sensitive requests must be immediately escalated to licensed human representatives. Clients may request a human representative at any time.

6. SMS/MMS TEXT MESSAGING & MOBILE DATA PRIVACY

- **Program Scope:** Text messages are used for quote updates, appointment reminders, policy reviews, customer service, and optional promotional messaging.
- **Consent & Opt-In:** Marketing texts require prior express written consent obtained via an unchecked, affirmative checkbox on web forms. Marketing consent is never a condition of purchasing insurance. We maintain records of phone numbers, timestamps, consent mechanism text, and source URLs for audit compliance.
- **Mobile Information Non-Sharing:** No mobile information or SMS opt-in data will be sold, rented, or shared with third parties or affiliates for their marketing or promotional purposes.
- **Opt-Out & Support:** Clients can reply STOP to any text to revoke consent immediately. Reply HELP or call (810) 209-4800 for assistance.

7. ADMINISTRATIVE, PHYSICAL, & TECHNICAL SAFEGUARDS

A. Administrative Safeguards

- **Privacy & Security Official:** Douglas B. McCullough is designated to oversee policy implementation and compliance.
- **Workforce Training:** All new associates must complete HIPAA and privacy training within sixty (60) days of hire, with periodic refresher training conducted as needed. Signed attestations are maintained.
- **Access Control & Termination:** System access is role-based and immediately revoked upon associate termination or role change.
- **Risk Analysis:** Periodic technical evaluations and security risk assessments are conducted internally and via external vendors.

B. Physical Safeguards

- **Facility Controls:** Visitor access is strictly controlled; visitors must be accompanied by an associate at all times.
- **Workstation & Document Security:** Workstations must be locked or logged off when unattended. Workstation screens are positioned to block visitor view.
- **Physical File Protection:** Physical documents containing PHI/NPI must be secured in locked file cabinets overnight or when unattended for over 30 minutes.

- **Disposal & Transport:** Hardcopy records designated for disposal must be placed in locked bins for shredding by a contracted vendor. Transported documents must be secured in sealed envelopes or locked containers. Degaussing and physical destruction are required for discarded digital media.

C. Technical Safeguards

- **Transmission Security:** Sensitive records (SSNs, banking details, full medical records) must never be sent over unencrypted SMS. All outgoing emails containing PHI must be encrypted or password-protected.
- **Facsimile Controls:** Outgoing faxes containing PHI require a standard cover sheet with a mandatory confidentiality disclaimer.
- **Authentication:** Multi-field authentication and user identification tracking are enforced before granting access or releasing records. Password-protected screen savers auto-activate during inactive sessions.

8. INDIVIDUAL PRIVACY RIGHTS & PROCEDURES

Clients and individual data subjects possess specific legal privacy rights:

- **Right of Access & Copying:** Requests to review or receive copies of PHI must be answered within thirty (30) days.
- **Right to Amendment:** Requests to correct inaccurate or incomplete PHI must be processed within sixty (60) days.
- **Right to an Accounting of Disclosures:** Individuals may request a log of non-routine disclosures made over the preceding six (6) years.
- **Restrictions & Alternate Communications:** Requests for confidential communications via alternative addresses or channels will be accommodated where reasonable.
- **Filing Complaints:** Individuals may submit written privacy complaints to the Agency Privacy Official or the Secretary of the U.S. Department of HHS. Complaints received on behalf of a Covered Entity will be forwarded immediately.

9. INCIDENT REPORTING & BREACH NOTIFICATION

- **Internal Reporting:** All associates and contractors must immediately report suspected or actual security incidents and privacy breaches to the Privacy & Security Official.
- **Assessment & Covered Entity Notice:** The Privacy Official will promptly investigate the incident, evaluate potential harm, and notify affected Covered Entities within the timeframe mandated in the applicable BAA (without unreasonable delay).
- **Mitigation & Retention:** The Agency will collaborate with Covered Entities on mitigation, regulatory notifications, and corrective actions. All incident logs and investigatory files must be retained for at least six (6) years.

10. DOCUMENT RETENTION & CONTRACT TERMINATION

- **Retention Schedule:** All documents, electronic records, consent logs, and incident files containing PHI or NPI will be retained for a minimum of six (6) years in compliance with federal HIPAA standards, or longer as mandated by Michigan insurance regulations.
- **Contract Termination (PHI Disposition):** Upon termination of a BAA or contract with a Covered Entity, the Agency will contact the Covered Entity to execute the return or secure destruction of all PHI. If immediate return/destruction is infeasible, protections will be extended until disposal is complete.

11. WORKFORCE SANCTIONS & AGREEMENTS

Compliance with this policy is a condition of employment and contract performance. Violations will result in disciplinary sanctions up to immediate termination, legal action, and potential civil or criminal penalties.

A. Associate Confidentiality Agreement

Associates acknowledge that all business records, client lists, and medical data are exclusive agency property. Confidentiality obligations continue indefinitely after employment terminates. Departing associates must surrender all devices, files, and physical property.

B. Third-Party / Vendor Nondisclosure Agreement

Contractors, consultants, and subcontractors with access to PHI/NPI must execute a written NDA or BAA restricting data use solely to contracted duties, enforcing non-disclosure, and requiring written certification of data destruction upon relationship termination.

12. POLICY REVISIONS & CONTACT INFORMATION

This policy is subject to periodic review and update to reflect statutory or technological changes. Updated versions will be published on the agency website with a revised effective date.

PRIVACY & SECURITY OFFICER CONTACT

Doug McCullough, Privacy & Security Official
McCullough Agency / Doug McCullough Insurance Agency LLC
2527 St. Clair River Dr., Algonac, MI 48001
Phone/Text: (810) 209-4800
Email: admin@mcculloughagency.com
Website: www.mcculloughagency.com