Settlement Administration Data Protection Checklist
Northern District of California

Limitation on Use of Data

- Affirmation that data provided to the administrator for purposes of notice, settlement, or award administration will be used solely for settlement implementation and for no other purpose

Technical Controls

- Firewalls and intrusion detection/prevention systems
- Endpoint detection and response (EDR) systems
- Complex password requirements
- Multi-factor authentication for access to systems and data
- Malware protection, anti-virus and vulnerability scanning and penetration tests
- Data encryption (including, "encrypted at rest and in transit," "scrambled in storage," and "cell- or column-level encryption for PII" protocols)
- "Key management" for access to encrypted databases (*e.g.*, using a hardware security module (HSM) or a key management service (KMS))
- Access only provided on need-to-know basis

Administrative Policies

- Personnel and support staff risk assessment and management, including pre-hire background checks and screening processes
- Personnel and support staff required to enter into non-disclosure and confidentiality agreements
- Access controls to systems and data, including guidance for granting, modifying, and reviewing access rights
- Information security and privacy policy trainings, including policy review, best practices, and data security
- No remote access to systems for employees
- Exit interviews/confirmation that terminated/departed employees are immediately cut off from access
- Robust audits of data privacy policies by third-party vendors
- Accreditation in accordance with ISO 27001 and SOC2 (among the industry standards listed below)
- Disclosure of external certifications and any notice of expiration

Crisis and Risk Management

- Incident response / "disaster plan" for immediate response to security incidents such as data breach
- Process and timing for notification to attorneys, claimants, and other stakeholders of a data breach and consideration of resources and/or remedies to provide thereto
- Vendor management program that determines and defines requirements to manage risk associated with outsourcing

Physical Access Controls

- Physical access security
    - Security guards

    - Access cards to facilities with assignment of identification card subject to approval and review
    - Logs of access
- Alarm systems
- CCTV recording systems

Data Collection and Retention

- Minimization of collection of personally identifiable information, *e.g.*, social security numbers and banking information
- Data collection only required to extent necessary for settlement administration
- Various methods for ensuring data protection and security
    - Data classification (including implementation of appropriate safeguards to protect from theft, loss, and/or unauthorized disclosure, use, access, destruction)
    - Compliance with applicable laws and regulations (see below)
    - Secure data transfer

Data Destruction

- Preservation of data only for so long as required for administration of the settlement and any relevant reporting required following the payments or distributions
- Secure data destruction (*e.g.*, 6 months – 1 year or when no longer required)
- Physical media (*e.g.*, paper, CDs) shredded or destroyed to point where they cannot be reconstructed
- Destruction of all derivative copies and/or back-ups

Applicable Laws, Standards, and Other Regulation

- Industry standards: National Institute of Standards and Technology (NIST), HIPAA, FISMA, System and Organization Controls (SOC1 and SOC2) or more advanced assessment, ISO 27001
- Local, national, international privacy regulations (including CCPA)

Ethical Rules

- Administrative policies and/or employee handbook incorporating commitment to ethical rules (*e.g.*, company, court ethical rules) setting forth standards of ethical and legal behavior
- Enforcement clauses, violation resulting in disciplinary action including and up to termination of employment

Customer Service Measures

- Description of settlement website and posting thereto of relevant privacy policies or statements (including portal for reporting suspected loss of confidential data submitted with claim)
- Explanation of role of claims administrator and how to prevent phishing (*e.g.*, clear indication that administrator will not request confidential information by e-mail and how to identify a valid e-mail sent from the administrator)