Unauthorized Disclosure and Incident Reporting

1. **Incident Reporting.**

    a. Business Associate shall report to Covered Entity the following:

        i. Any use or disclosure of PHI which is not in compliance with the terms of this Agreement or applicable law of which it becomes aware; and

        ii. Any security incident of which it becomes aware. For purposes of this Agreement, "security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

    b. Within 24 hours of discovery of a suspected reportable incident as described in 6.1.1 above, Business Associate shall notify Covered Entity of the existence and nature of the incident as understood at that time. Business Associate shall immediately investigate the incident and within 72 hours of discovery shall provide Covered Entity, in writing, a report describing the results of Business Associate's investigation, including:

        i. What data elements were involved, the extent of the data involved in the incident, and the identification of affected individuals, if applicable;

        ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI, or to have been responsible for the incident;

        iii. A description of where the PHI is believed to have been improperly transmitted, sent, or utilized, if applicable;

        iv. A description of the probable causes of the incident;

        v. A description of the proposed plan for preventing similar future incidents, including ongoing risk remediation plan approval; and

        vi. Whether the Associate believes any federal or state laws requiring notifications to individuals are triggered.

c. Reporting and other communications made to the Covered Entity under this section must be made to the agency's HIPAA privacy officer at:

HIPAA Privacy Officer
Office of Legal Counsel
The Ohio Department of Medicaid
50 West Town Street
Columbus, Ohio 43215
Phone: 614-752-3690
PrivacyOffice@medicaid.ohio.gov

2. **Business Associate Mitigation.** In addition, Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement, and report its mitigation activity back to the agency. Business Associate shall preserve evidence.

3. **Coordination.** Business Associate will coordinate with the agency to determine additional, specific actions that will be required of the Business Associate for mitigation of the Breach, which may include notification to the individuals, entities or other authorities. Notifications, if any, will be made at the direction of the agency.

4. **Incident costs.** Business Associate shall bear all costs associated with the incident. This may include, but not be limited to, costs associated with notifying affected individuals. It also may include the cost of investigation, remediation, and assistance to individuals including services such as a standard level of identity-theft protection service that includes credit-monitoring such as AllClear ID's standard service with credit monitoring or other comparable service available to Ohio agencies under state term schedules.

5. **Agency Indemnification.** Business Associate hereby indemnifies Agency and agrees to hold Agency harmless from and against any and all losses, expense, damage or injury that Agency may sustain as a result of, or arising out of, Business Associate, or its agent's or subcontractor's, unauthorized use or disclosure of PHI.