Data Security and Privacy Incident Response Policy

Policy Statement

The intent of this policy is to provide a structured and systematic incident response process to report suspected thefts involving data, data breaches or exposures (including unauthorized access, use, or disclosure) that affect Biomedical Research Models Inc. d/b/a Biomere, to appropriate individuals; and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved.

Policy Content

Data security and privacy incidents must be reported, identified, responded to, remediated, and resolved. Detailed requirements for each of these steps are below.

Incident Response Procedures

(i) Detection and Discovery – Biomere shall develop, implement, and maintain procedures to detect, discover, and assess potential information security incidents through automated means and individual reports.

(a) Automated Detection. Biomere shall develop, implement, and maintain automated detection means and other technical safeguards as described in its Automated Detection Statement.

Examples

- User accesses system or application with credentials other than his/her own.
- Unauthorized access to a system, application, or document.
- A rogue device is connected to the network which impacts or prevents others from working.
- System or individual device is infected with malware or phishing (e.g., virus, ransomware).
- Potential data loss due to a malware infection.

(b) Reports from Employees or Other Internal Sources. Employees, or others authorized to access Biomere's IT systems, network, or data, shall immediately report any actual or suspected information security incident to Director, Accounting ("Privacy Officer"). Individuals should report any information security incident they discover or suspect immediately and must not engage in their own investigation or other activities unless authorized.

Examples

- Client information is misdirected or disclosed via mail, fax, verbal means.
- Client documents are misplaced, stolen, or lost.
- Documents are exposed (e.g., files left open on computer), improperly disposed of (e.g., not shredded) or stored (e.g., not locked or protected).
- User accesses system or application with credentials other than his/her own.
- Unauthorized access to a system, application, or document.
  A device (e.g., laptop, smartphone, desktop, tablet, removable storage, smart watches, cameras, voice recorders, etc.) containing client data is lost, stolen, or otherwise unaccounted for.

(c) Reports from External Sources. External sources who claim to have information regarding an actual or alleged information security incident should be directed to Director, Accounting. Employees who receive emails or other communications from external sources regarding information security

incidents that may affect Biomere or others, security vulnerabilities, or related issues shall immediately report those communications to the Privacy Officer and shall not interact with the source unless authorized.

(d) Assessing Potential Incidents. Upon notification of a potential security and privacy incident, IT department under the supervision of the Privacy Officer shall promptly assess and gather information to determine the impacted data, systems, and business processes.

(ii) Escalation. Following identification of an information security incident, the IT department under the supervision of the Privacy Officer, shall perform an initial risk-based assessment and determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to Biomere and its Customers, employees, or others.

Based on the initial assessment, the information security coordinator, or a designate, shall:

(a) Initial Notifications. Notify (if necessary) organizational leadership and any applicable business partners or service providers, Biomere's cyber insurance carrier, and law enforcement or other authorities (see Section (vi), Communications and Notifications).

(b) Determine Decision-Making Authority. Following initial notifications, work with organizational leadership (if necessary) to establish any decision-making authority levels according to the information security incident's specific facts and circumstances.

(iii) Incident Follow-up. IT department under the supervision of the Privacy Officer will develop a security incident report summarizing the security and privacy incident and outlining recommended actions.

(iv) Containment, Remediation, and Recovery. Next, the Privacy Officer shall direct execution of the response plan the IT Department has formulated according to its incident investigation and analysis to contain, remediate, and recover from each identified information security incident, using appropriate internal and external resources.

(v) Evidence Preservation. The Privacy Officer shall direct appropriate internal or external resources to capture and preserve evidence related to each identified information security incident during investigation, analysis, and response activities. The Privacy Officer shall seek counsel's advice, as needed, to establish appropriate evidence handling and preservation procedures and reasonably identify and protect evidence for specific information security incidents.

(vi) Communications and Notifications. For each identified information security incident, the Privacy Officer shall determine and direct appropriate internal and external communications and any required notifications. Only the Privacy Officer may authorize information security incident-related communications or notifications. The Privacy Officer shall seek counsel's advice, as needed, to review communications and notifications targets, content, and protocols.

(a) Internal Communications. Working with appropriate legal, compliance and public relations groups, Privacy Officer shall prepare and distribute any internal communications he or she deems appropriate to the characteristics and circumstances of each identified information security incident.

(i) Organizational Leadership. The Privacy Officer shall alert organizational leadership to the incident and explain its potential impact on Biomere, its customers, employees, and others as details become available.

(ii) General Awareness and Resources. As appropriate, the Privacy Officer shall explain the incident to Biomere's employees and other stakeholders and provide them with resources to appropriately direct questions from customers, media, or others.

(b) External Communications. Working with appropriate legal, compliance and public relations groups, Privacy Officer shall prepare and distribute any external communications he or she deems appropriate to the characteristics and circumstances of each identified information security incident.

(i) Public Statements. If Biomere determines that external statements are necessary, the Privacy Officer shall provide consistent, reliable information to the media and public regarding the incident using Biomere's website, press releases, or other means.

(ii) Law Enforcement. The Privacy Officer shall report criminal activity or threats to applicable authorities, as Biomere deems appropriate.

(c) Notifications. While the Privacy Officer may choose to authorize discretionary communications, certain laws, regulations, and contractual commitments may require Biomere to notify various parties of some information security incidents. If applicable to a specific information security incident, as required, the Privacy Officer shall:

(i) Authorities. Notify applicable regulators, law enforcement, or other authorities.

(ii) Affected Individuals. If an applicable breach of personal information occurs, prepare and distribute notifications to affected individuals.

(iii) Cyber Insurance Carrier. Notify Biomere's cyber insurance carrier according to the terms and conditions of its current policy, including filing a claim, if appropriate.

(iv) Others. Notify customers or business partners according to current agreements.

(vii) Post-Incident Review. At a time reasonably following each identified information security incident, the Privacy Officer shall reconvene the team who participated in response to the incident, and affected work group representatives, as appropriate, as a post-incident review team to assess the incident and Biomere's response.

(a) Review Considerations. The post-incident review team shall consider Biomere's effectiveness in detecting and responding to the incident and identify any gaps or opportunities for improvement. The post-incident review team shall also seek to identify one or more root causes for the incident and, according to risk, shall recommend appropriate actions to minimize the risks of recurrence.

(b) Report. The post-incident review team shall document its findings using the Incident Form.

(c) Follow-Up Actions. The Privacy Officer shall monitor and coordinate completion of any follow-up actions identified by the post-incident review team, including communicating its recommendations to and seeking necessary authorization or support from Biomere's leadership.

Policy Training and Testing

(i) Training. The Privacy Officer shall develop, maintain, and deliver training regarding this Policy that periodically, but at least annually:

(d) Informs all employees, and others who have access to Biomere's IT or other systems, network, or data, about the Policy and how to recognize and report potential information security incidents.

(e) Educates members of the IT department and any other members designated to the information security team on their duties and expectations for responding to information security incidents.

(ii) Testing. The Privacy Officer with the help of the IT Department and other internal or external teams shall coordinate exercises to test this policy periodically, but at least annually. The Privacy Officer shall ensure documentation of test results, lessons learned, and feedback and address them in policy reviews.

2. Policy Review. Biomere will review this IRP at least annually, or whenever there is a material change in Biomere's business practices that may reasonably affect its cyber incident response procedures. Plan reviews will also include feedback collected from post-incident reviews and training and testing exercises. The Privacy Officer must approve any changes to this Policy and is responsible for communicating changes to affected parties.