Data Breach Investigation and Mitigation Checklist

Actions to Be Taken Immediately upon Identification of an Incident

1. Notification Process
   - ☐ Notify privacy and security officers
   - ☐ Initiate security incident report form
   - ☐ Record name and contact information of reporter
   - ☐ Gather description of event
   - ☐ Identify location of event

2. Investigation Steps
   - ☐ Establish security incident response team (e.g., security officer, privacy officer, risk manager, administration, and others as needed) and identify team leader (e.g., privacy or security officer)
   - ☐ Identify and take immediate action to stop the source (e.g., hacking) or entity responsible (e.g., work force member, vendor)
   - ☐ Identify system, application, or electronic PHI compromised and then immediately begin identification process of those patients whose information was compromised and what data elements were included (e.g., name, age, date of birth, Social Security number, diagnosis)
   - ☐ Determine need to notify key internal stakeholders not represented on the team:
     - ▫ HIM department (if necessary to sequester records)
     - ▫ Billing and patient accounts department (if necessary to suspend billing process)
     - ▫ Human resources department (if a work force member is suspected)
     - ▫ Vendor relations or purchasing leadership
     - ▫ Others as necessary
   - ☐ Identify the source or suspects involved in event:
     - ▫ If the source is identified as a vendor or business associate, determine if business associate agreement has been established (collect as evidence)
     - ▫ If the source is identified as a work force member, establish existence of criminal background check, privacy and security education and training, etc. Coordinate with human resources to determine appropriate sanctions.
     - ▫ If the source is external, work with law enforcement agency to determine appropriate actions
   - ☐ Carry out IT forensic investigation to gather evidence and determine course of events as well as identify electronic PHI compromised
   - ☐ Identify and sequester pertinent medical records, files, and other documents (paper and electronic)
   - ☐ Determine need for external notification or involvement (see individual sections following):
     - ▫ Legal counsel (identify all communications as "Privileged and Confidential Attorney-Client Communication/Work Product")
     - ▫ IT forensics support
     - ▫ Law enforcement agency (local and federal)
     - ▫ Media
     - ▫ Victims
   - ☐ Determine need to contact other additional external stakeholders:
     - ▫ Corporate office
     - ▫ Licensing or accrediting agencies
     - ▫ Centers for Medicare and Medicaid Services, Office for Civil Rights (self-reporting is not required by regulation, it is an organizational decision)
     - ▫ Business associates or partners

Other Actions as Applicable

1. Contact Law Enforcement Officials
   - ☐ Verify event constitutes a crime and is reportable
   - ☐ Determine appropriate law enforcement agency and contact
   - ☐ In cooperation with local law enforcement officials, determine the need to involve other external law enforcement agencies (e.g., FTC, FBI, Social Security Administration, Inspector General)
   - ☐ Obtain name of law enforcement contact to provide upon victim request

2. Collection of Evidence
   - ☐ Security incidence response form
   - ☐ IT forensic evidence (e.g., reports, logs, audits)
   - ☐ Records of communications (e.g., phone logs, e-mail, letters)
   - ☐ Law enforcement agency and police reports
   - ☐ Legal counsel guidance

3. Notification of Victims
   - ☐ Determine need to notify victims. Consider:
     - ▫ Likelihood of harm (e.g., stolen laptop protected by password or encryption, PHI limited to first names and dates only)
     - ▫ Recipient of information, if known (e.g., if recipient is known covered entity, there is less risk than if PHI was disclosed to other individuals)
     - ▫ Regulatory reporting and disclosure requirements (review state regulations)
     - ▫ Type of incident (e.g., targeted theft of data or incidental as part of crime of opportunity such as laptop left unaccompanied in airport waiting area)
     - ▫ Actions of other organizations if involved in event (e.g., information system of vendor hacked containing multiple healthcare clients)
     - ▫ Historical responses by others involved in similar events
   - ☐ Prepare a communication plan to cover oral and written communications to victims as well as information to assist them with personal needs (FTC guidance) and organizational contact person for questions and concerns (privacy officer)
   - ☐ Provide information regarding law enforcement contacts
   - ☐ Consider provision of credit monitoring services (e.g., fees paid by organization? If so, how long?)

Data Breach Investigation and Mitigation Checklist

Actions to Be Taken Immediately upon Identification of an Incident

4. Communication with Media
   - ☐ Determine need to proactively contact media or prepare press release in response to inquiries. Consider:
     - ▫ Likelihood of media awareness or investigation
     - ▫ Scope of event (e.g., number of individuals impacted, type of information disclosed, threat of harm to victims)
     - ▫ Potential for harm to individuals (e.g., patients, business associates, clients, others)
     - ▫ Organizational preventive safeguards and practices
     - ▫ Mitigation efforts
     - ▫ Preparation of talking points for public affairs department outlining organizations privacy and security safeguards
     - ▫ Limitations of disclosure as advised by legal counsel or law enforcement

5. Other Organizational Processes to Be Considered
   - ☐ Determine how best to account for disclosures of PHI (HIPAA requirement):
     - ▫ Update each health record (paper or electronic) with disclosure information
     - ▫ Provide list of patients to privacy officer in response to accounting of disclosure requests (may be preferred for large numbers of disclosures)
   - ☐ If event is result of a business associate's failure to safeguard PHI, consider need to terminate relationship (refer to business associate agreement)

Follow-Up Activities, Identifying Opportunities for Improvement

1. Evaluation of Security Incident Response (Document on Form)
   - ☐ Identify actions:
     - ▫ Identification measures (incident verified, assessed, options evaluated)
     - ▫ Evidence collected
     - ▫ Eradication measures
     - ▫ Recovery measures
   - ☐ Determine:
     - ▫ How well did the work force members respond to event?
     - ▫ Were documented procedures followed? Were they adequate?
     - ▫ What information was needed sooner?
     - ▫ Were there any steps or actions that might have inhibited recovery?
     - ▫ What could work force members do differently the next time an incident occurs?
     - ▫ What corrective actions can prevent similar events in the future?
     - ▫ What additional resources are needed to detect, analyze, and mitigate future incidents?
     - ▫ Can missing electronic PHI be recreated to provide continuity of care?
     - ▫ What external resources and contacts proved helpful?
     - ▫ Other conclusions or recommendations

2. Follow-Up
   - ☐ Security incident response form completed and supporting documentation made part of form or filed as attachments (consider restricting access to the form)
   - ☐ Policy and process review completed and all necessary changes made based on shortcomings identified through managing event
   - ☐ Training, education, and awareness activities carried out (balancing need for awareness with disclosure of event)
   - ☐ Event documented as educational case study (de-identified) for internal use

3. Other
   - ☐ Consider the offer of a reward for return of lost or stolen equipment ❖