COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 30, Number 40. November 08, 2021

Data Breach Checklist

By Nina Youngstrom

With the escalation of cyberattacks, health care organizations should have an incident response plan in place, according to attorneys at Morgan Lewis who developed this data breach checklist. They won't have time to plan when a ransomware attack or other breach is underway, according to Scott Memmott, Mark Krotoski, and Reece Hirsch. The attorneys recommend tabletop drills, where hospitals "dream up a worst-case scenario and simulate what decision-makers would do and assess the level of preparation," Hirsch said. Contact Krotoski at mark.krotoski@morganlewis.com, Memmott at scott.memmott@morganlewis.com and Hirsch at reece.hirsch@morganlewis.com.

PHASE I: ALERT AND ORGANIZATION

1. Company alerted to possible data breach—record date, time, and method of alert
2. Notify internal Incident Response Team (IRT), consisting of a representative from
    a. Information Technology
    b. Legal/Compliance
    c. Outside Counsel (Morgan Lewis)
    d. Human Resources
    e. Public Relations
    f. Customer Service
    g. Executive
3. Identify an Incident Lead for this incident—performs as project manager
4. Contact outside counsel at Morgan Lewis
5. Convene conference call of IRT
6. Consider hiring forensic technology partner depending on available internal resources and complexity of breach
7. Notify insurance carrier/understand scope of preauthorization or limitations on third-party vendor reimbursement
8. Check with counsel on proper role and implementation of the attorney-client privilege in the data breach investigation

PHASE II: INITIAL SCOPING BEFORE CONTAINING AN ONGOING BREACH

1. Identify, document, and preserve scope of compromise to the extent possible within 24–48 hours
2. Consider notifications or steps to take before stopping the breach that may prevent harm in the event the act of stopping the breach alerts data thieves that you have discovered them
3. Preserve any evidence related to the ongoing breach

PHASE III: CONTAIN THE BREACH

1. Be sure that the full scope of compromise is understood to the extent possible within 24–48 hours
2. Contain/arrest the breach—stop any possible flow of data to unauthorized recipients
3. Document results of containment effort

PHASE IV: INVESTIGATION

1. Root cause analysis
2. Classify type of breach
    a. Hacking
    b. Internal
    c. Loss/theft of tangible data (computer, device, storage media)
    d. Inadvertent disclosure
    e. Loss with no known disclosure
    f. Other
3. Full identification of data compromised
    a. Type of information compromised
        i. Sensitive personal information
            1. Social Security numbers
            2. Credit card information
            3. Financial account data
            4. Medical information
            5. Usernames and passwords
            6. Driver's license numbers
            7. Other sensitive personal information (disclosure of which could cause harm)
        ii. Other personal information

1. Contact information (name, address, email address, phone number, etc.)
2. Preferences, purchase history
3. Other information linked to a person that is not sensitive

b. Individuals whose information was compromised, including where they reside

4. Determine nature of any unauthorized recipients
    a. Employee acquisition in good faith
    b. Business partner
    c. Trustworthy recipient who normally receives information of this nature
    d. Unknown individuals, but definite disclosure
    e. Lost information—may not have been disclosed
    f. Suspected bad actor/employee not in good faith
    g. Known bad actor/departed or departing employee
5. Assess known or discoverable actual use of compromised information
6. Undertake security updates necessary before notification

PHASE V: NOTIFICATIONS (IN LIGHT OF INFORMATION DEVELOPED IN PHASE IV)

1. Before notifications
    a. Develop public relations plan for potential media inquiries
    b. Consider notification to company board of directors or others who should be notified before public
    c. Prepare for inquiries from affected individuals—call center or other
2. If criminal and depending on seriousness and other factors, notify law enforcement—local, FBI, Secret Service, or other
3. If required by law or recommended because individuals could do something to prevent further harm to themselves, make notifications to affected individuals. If made,
    a. Include what happened, what the company has done, and what the individual can do to prevent any harm
    b. Include legally required information and resources available from government agencies
    c. Consider an offer of identity theft prevention/credit monitoring depending on nature of information compromised
4. Notifications to government agencies and Attorneys General as required by law

5. Other notifications as required by information at issue
6. Evaluate feedback from notifications and determine if additional steps/notifications are required

PHASE VI: POST-NOTIFICATIONS

1. Disclosures to investors, stockholders, Securities and Exchange Commission, securities disclosures, etc.
2. Cost recoveries—responsible third parties, insurance, other
3. Consider longer-term security upgrades or other measures to prevent reoccurrence or similar events
4. Analyze data breach notification plan/checklist for necessary changes in light of lessons learned
5. Prepare final reports
    a. Executive report with a summary of what happened, how it was addressed, what notifications were provided, and steps taken to prevent future incidents of the same or similar nature
    b. Technical report with detailed background of the event; evidentiary backup for analysis, decisions, and conclusions; and evidence of preventative measures

REMINDERS

- Maintain confidentiality—update IRT and executives frequently; other disclosures only to those who need to know
- Preserve evidence and information for future investigations
- Document events with dates and times; record reasons for determinations made
- The European Union General Data Protection Regulation has a 72-hour deadline for some notifications; check early with outside counsel about whether it applies and how to manage it.