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