Appendix A: Additional Discussion Questions

Cyber Preparedness and Planning

1. What level of funding and/or resources are devoted to cyber preparedness? Based on your risk assessment, what is the range of potential losses from a cyber incident?
2. What external reviews or audits of your IT plans, policies, or procedures have been conducted within the last year?
3. What role does organizational leadership play in cybersecurity?
4. How well defined is cybersecurity in relation to contracts with third-party support vendors and crucial suppliers?
    a. How often are contracts reviewed?
    b. How well do your contracts address incident response?
5. How would your facility's employees be able to distinguish between normal and abnormal traffic?
6. What type of hardware and/or software does <Organization> use to detect/prevent malicious activity of unknown origin on <Organization> systems/network?
7. How are employees trained to recognize and report cyber threats such as phishing scams?
    a. What additional training does <Organization> require for those who fall for a fake phishing campaign?

Information Sharing

1. What established mechanisms does the facility have to facilitate rapid information dissemination?
    a. What are the known communication gaps at your facility? Who is responsible for addressing those gaps?
2. What other sources of cybersecurity threat intelligence does the clinic receive (e.g., information from FBI, H-ISAC, HHS, open-source reporting, security service providers)?
    a. What cyber threat information is most useful, timely, and actionable?
    b. Who is responsible for collating/disseminating information across <Organization>?
3. What are some challenges that are experienced by information technology and business continuity planning in terms of information sharing? Is information flowing in both directions?

Incident Response

1. When was your facility's cybersecurity incident response plan issued, and when was the plan last revised?
2. What key contact information is included in the incident response plan if you suspect you have experienced a cyber incident?
3. When do your IT and helpdesk staff conduct network maintenance (e.g., specific days or times of day)?
4. How would these events affect your facility's business operation/processes?
5. What risk assessments are performed on all servers on the network?
    a. What processes exist to evaluate each server's criticality and applicability to software patches?
6. What resources and capabilities are available to analyze an intrusion or mitigate the incident?
    a. Internally?
    b. Through the private sector (third-party vendors)?

    c. Through government partners?
7. Describe the decision-making process for protective actions in a cyber incident.
    a. What options are available?
    b. What options are documented in plans?
    c. How are they activated?
8. What immediate protection and mitigation actions would be taken at your facility in this scenario? Who is responsible for those actions?
9. How would your organization respond to the discovery of a malicious, unauthorized administrator account on your systems? Who would be informed internally? Who would be informed externally (e.g., law enforcement, cybersecurity insurance partners, etc.)?
10. What detection methods does the facility have to identify a compromise?
11. What protective actions would you take across non-impacted systems in the scenario presented?
    a. Who is responsible for protective action decision-making?
    b. How are actions coordinated across parts of the facility?
12. How would you rate this security incident severity for your facility? What additional notifications or actions would this prompt?
13. Describe whether this scenario exceeds your facility's ability to respond.
    a. If so, what are the established procedures to request additional support?
14. Who does your clinic receive cyber response technical assistance from?
    a. What plans and procedures exist to access this assistance?
15. What service provider relationships are needed for incident/breach response issues (e.g., credit counseling, forensic/computer security services)?
    a. What are some challenges that are experienced by information technology and business continuity planning in terms of information sharing? Is information flowing in both directions?
16. What alternative systems or manual processes are available to continue operations if a critical system is unavailable for a significant period?
    a. Who can authorize use of alternate systems or procedures?
17. When and how does your facility determine a cyber incident is closed?
18. What are your defined cybersecurity incident escalation criteria, notifications, activations, and/or courses of action?
    a. Where does this incident fall within the incident severity schema for your facility?
    b. When would leadership be notified?
19. What incident de-escalation procedures are in place?
    a. What quantifiable, repeatable process exist for determining when an incident is resolved and when the incident response team can stand down?
20. Describe your facility's After-Action Report or lessons learned process.
    a. Who leads this process for a cyber incident?
    b. How are recommended improvements implemented and tested?
21. What remediation is required of employees to ensure an event like this does not happen again (training, self-education, etc.)?

Ransomware

1. What resources are required for incident investigation and attribution?
2. If you were one of the individuals who received the ransom demand, who would you inform, internally? Who would you inform externally?
3. How is ransomware addressed in your incident response plan?
    a. How frequently does your facility exercise your response to ransomware?
4. What formal policies and procedures does your facility have to document the process for restoring backed-up data?
    a. How does your facility ensure the integrity of backed-up data before restoration?
5. What processes and resources are used for evidence preservation and forensics?
    a. When would your facility engage law enforcement, if at all?
    b. Who would your facility be contacting from local, state, and federal entities?

Training and Exercises

1. How do employees report suspected phishing attempts?
    a. What actions does your facility take when suspicious emails are reported?
    b. What formal policies or plans would be followed?
    c. What training do employees receive on phishing (e.g., phishing self-assessments)?
2. What basic cybersecurity and/or IT security awareness training does your organization provide to all users (including managers and senior executives)?
    a. How often is training provided?
    b. What topics are covered in your training?
    c. What training is required to obtain network access?
    d. What security-related training does your department or agency provide to, or contractually require of, IT personnel and vendors with access to your organization's information systems? How often do they receive the training?
3. What special training, if any, do your cybersecurity incident response team members undergo to detect, analyze, and report this activity? Describe this training.
    a. How is your staff trained to read and analyze your intrusion detection system logs?
4. What are your cybersecurity incident response team's exercise requirements?
5. How does your organization's efforts address both physical and cyber risks?
6. Describe the level of involvement and participation of senior or elected officials in your cybersecurity exercises.
7. What are the additional training and/or exercising requirements for your facility?

Data Exfiltration

1. What actions would be taken when the exfiltration is discovered? Does your facility have written plans that would be implemented?
2. What impact will the potential sale of patient-sensitive or PHI have on the facility's response and recovery activities?
    a. What is IT's reporting process?
    b. How have your public relations priorities changed?

    c. What additional legal or regulatory notifications are required?

Public Affairs

1. What steps would be taken to address the public following these cyber incidents?
    a. How would patients be notified about the cyberattacks?
2. What online resources and communication formats does your facility use to keep patients, families, and the public informed regarding any incidents?
3. How would your organization respond to the emerging news and social media issues?
    a. What communications processes would be used for immediate release of messages? Does your organization have pre-approved messages?

Legal

1. What are the legal issues your facility must address?
2. What legal documents should your organization have (e.g., with third-party vendors)?
3. What is the role of the legal department in this scenario?
4. What are your facility's security breach notification laws? What do they include?
5. What security breach notification laws does your state have? What do these laws include?
6. What processes exist to collect evidence and maintain the chain of custody?