Cybersecurity for Health Care Providers

Montgomery County Medical Society Provider Meeting

February 28, 2017

The MARYLAND
HEALTH CARE COMMISSION

Overview

- Cybersecurity defined
- Cyber-Threats Today
- Impact of Cybersecurity to Health Care
- Protecting Against Cyber-Attacks
- Overview of the Maryland Health Care Commission (MHCC) Cybersecurity Self-Assessment Tool (tool)
- Use of the tool
- Review of the tool and feedback discussion

Cybersecurity

- The technology, processes, and practices that protect networks, computers, programs, and data from attack, damage, or unauthorized access
- Requires coordination of many different elements, including:
  - Securing all networks, information, and health information technology (IT) system(s);
  - Disaster recovery and business continuity planning; and
  - End-user education

Cyber-threats Today

- Technology is no longer limited to the home or office and has been increasingly integrated into our everyday lives
- Cyber-risk landscape is constantly changing making cybersecurity a challenge
- There are two main types of approaches hackers can use to initiate a cyber-attack
  - External: Initiated from outside the network, such as a malware delivery through a phishing attempt or web server hacks, to execute a computer intrusion
  - Internal: Initiated through the action of a willing or unknowing person, such as inserting a flash drive into a computer

Impact to Health Care

- Cyber-attackers are increasingly targeting health care
  - Puts at risk patient information, intellectual property, sensitive business information, operational dependencies, and the practice's reputation
- Patient records are worth more on the black market than a social security number because they are a "one stop shop" of information desired by hackers
- Damage from a stolen record can take years to repair
- Other devices can also be attacked to gain access to the practice's network
  - A hacker can gain control of networked medical devices, such as insulin pumps and blood pressure machines, and use this to navigate through the network to access other devices, such as computers.

Protecting against Cyber-attacks

- The health care sector is slow to detect fraud, unlike the financial sector that can quickly detect fraud and block compromised data accessed
- Implementing cybersecurity best practice safeguards is complex, which can put a burden on providers with limited resources
- A key step for providers to take to protect against a cyber-attack is to assess existing processes and procedures to identify gaps in cybersecurity
- Providers can develop processes to address existing gaps to protect against and mitigate the effects of a cyber-attack
- Ongoing assessments helps providers evaluate progress in developing processes to address gaps, as well as continuously assess the adequacy of processes to protect against new cyber-threats

Cybersecurity Self-Assessment Tool

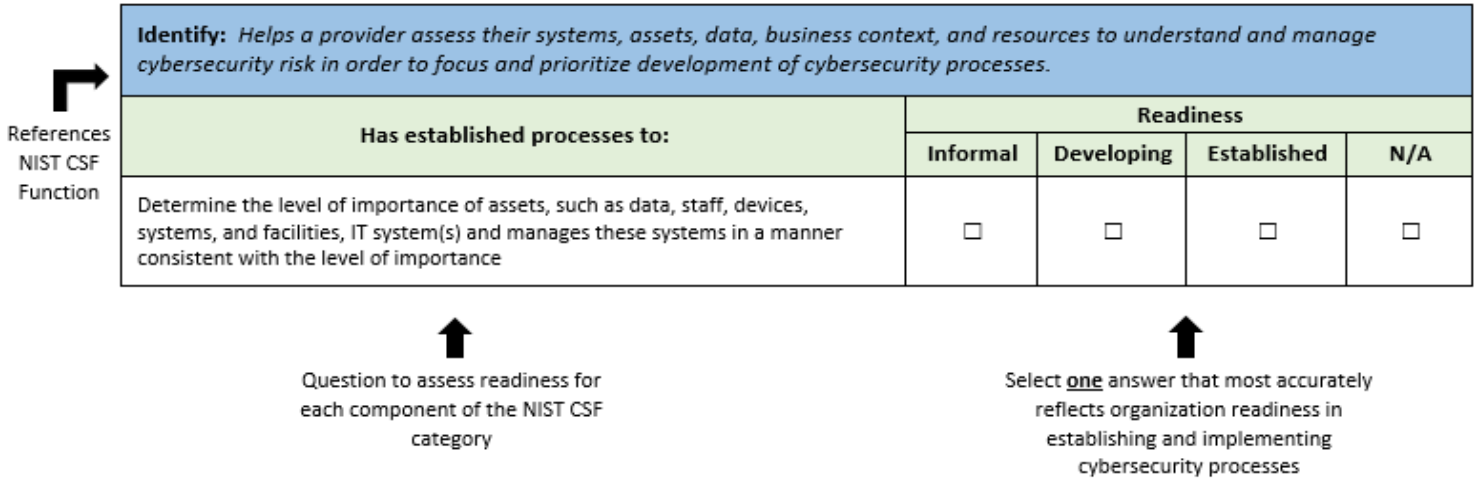
- The *Cybersecurity Self-Assessment Tool* (tool) was developed by MHCC with stakeholder input to assist providers in assessing their practice's cybersecurity processes
  - Helps providers gain an understanding of their overall cybersecurity readiness and provides an overview of a practice's cybersecurity environment
- Uses industry standards and best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
  - Addresses five core functions, Identify, Protect, Detect, Respond, and Recover, identified through a collaboration of industry experts to be in line with existing industry standards, guidelines, and practices for addressing cybersecurity

How the Tool Can Help Your Practice

- Assist providers in strengthening their IT system(s)
- Use results to inform work in developing cybersecurity protections by
  - Identifying gaps in the current cybersecurity environment
  - Modifying existing cybersecurity processes
  - Developing and implementing best practices to protect health information that is stored, transmitted, or maintained electronically

How to use the Tool

- **Select the answer choice that reflects the practice's readiness to establish and implement the cybersecurity processes for each of the following items:**
  - ***Informal:*** **No formal processes exist**
  - ***Developing:*** **Formal processes are in development**
  - ***Established:*** **Formal processes that are standardized throughout the practice have been established**
  - ***N/A:*** **Not applicable to the practice**



Scoring

- Responses for each section are tabulated
- A "Readiness Percent" score is calculated by dividing the number established by the total questions answered
- This number is then used as an indicator of the practice's overall readiness

Readiness Indicator											
Readiness Percent	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
	Partial				Moderate					Advanced	

Feedback on the tool

- We will walk through completing each of the sections of the tool
- Conduct an open group discussion after each section
- Aim to gain feedback on the utility of the tool and answer the following questions:
  - How applicable is the information to your practice?
  - Is the information easy to use and understand?
  - Is the information helpful in assessing the cybersecurity environment at your practice?
  - Does the scoring accurately reflect the level of cybersecurity readiness at your practice?

Identify: *Helps a provider assess their systems, assets, data, business context, and resources to understand and manage cybersecurity risk in order to focus and prioritize development of cybersecurity processes.*					
#	**Has established processes to:**	**Readiness**			
		Informal	**Developing**	**Established**	**N/A**
1	Determine the level of importance of assets, such as data, staff, devices, systems, and facilities, IT system(s) and manages these systems in a manner consistent with the level of importance	☐	☐	☐	☐
2	Prioritize the practice's activities and workflows to inform cybersecurity roles, responsibilities, and risk decisions	☐	☐	☐	☐
3	Manage and monitor IT system(s) operational, environmental, and regulatory requirements to inform and manage cybersecurity risk	☐	☐	☐	☐
4	Identify, document, and evaluate IT system(s) vulnerabilities, internal and external threats, and business impacts on operations	☐	☐	☐	☐
5	Identify IT system(s) priorities, constraints, risk tolerances, and assumptions, and use this to support risk decisions	☐	☐	☐	☐

Protect: *Provides the framework for providers to develop and implement the appropriate safeguards to limit or contain the potential impact of an IT system(s) cybersecurity event.*					
#	**Has established processes to:**	**Readiness**			
		Informal	**Developing**	**Established**	**N/A**
1	Limit access to IT system(s) and facilities to authorized users, devices, activities, and transactions	☐	☐	☐	☐
2	Educate and train staff on cybersecurity awareness necessary to perform information security related duties	☐	☐	☐	☐
3	Manage IT system(s) data to protect confidentiality, integrity, and availability of electronic protected health information	☐	☐	☐	☐
4	Develop and maintain IT system(s) security policies, processes, and procedures to adequately protect IT system(s)	☐	☐	☐	☐
5	Conduct and document all manufacturer recommended maintenance and repairs for IT system(s)	☐	☐	☐	☐
6	Manage the security of IT system(s) through the establishment of standardized policies, procedures, and agreements	☐	☐	☐	☐

Detect: *Assist the practice to perform an assessment of processes to rapidly identify an IT system(s) cybersecurity event, test detection processes, analyze data to understand cybersecurity attack targets and methods, and utilize assessment results to inform improvements to practice processes.*					
#	**Has established processes to:**	**Readiness**			
		Informal	**Developing**	**Established**	**N/A**
1	Detect unusual activity in the IT system(s) in a timely manner, analyze the potential impact(s) of a cyber event, and establish incident alert levels	☐	☐	☐	☐
2	Routinely monitor IT system(s), the physical environment, and staff to identify potential cybersecurity events	☐	☐	☐	☐
3	Assess IT system(s) to detect unusual events in a timely and appropriate manner, and take the necessary action to minimize risks of any unusual event(s)	☐	☐	☐	☐

Respond: *Assists providers containing the impact of a potential IT system(s) cybersecurity event by assessing the current processes in place to respond to a detected IT system(s) cybersecurity event.*					
#	**Has established processes to:**	**Readiness**			
		Informal	**Developing**	**Established**	**N/A**
1	Respond to detected IT system(s) cybersecurity events in a timely manner	☐	☐	☐	☐
2	Coordinate IT system(s) cybersecurity response activities with internal and external stakeholders, including training of staff, reporting of events, sharing of information, and coordinating with stakeholders as necessary	☐	☐	☐	☐
3	Analyze and categorize IT system(s) cybersecurity response activities to ensure appropriateness and the ability to support recovery	☐	☐	☐	☐
4	Contain, reduce the effects of, and eliminate an IT system(s) cybersecurity event	☐	☐	☐	☐
5	Make improvements to existing IT system(s) cybersecurity response processes through the application of lessons learned from detection and response activities	☐	☐	☐	☐

Recover: *Supports providers in rapidly recovering and mitigating the impact of an IT system(s) cybersecurity event by assessing the processes to support restoration of services impacted during an IT system(s) cybersecurity event.*					
#	**Has established processes to:**	**Readiness**			
		Informal	**Developing**	**Established**	**N/A**
1	Recover from cybersecurity events to ensure IT system(s) are restored in a timely manner	☐	☐	☐	☐
2	Incorporate lessons learned from an IT system(s) cybersecurity event into the operations and update recovery plans	☐	☐	☐	☐
3	Coordinate IT system(s) restoration activities with internal and external parties as deemed appropriate by the provider	☐	☐	☐	☐

Thank You!

For more information or questions please contact:

Justine Springer

justine.springer@maryland.gov

410-764-3777

The MARYLAND
HEALTH CARE COMMISSION