Form Approved
OMB No. 0990-0379
Exp. Date 09/30/2020

HHS FOCUS GROUPS
Discussion Guide – Version 5
May 1, 2018

I. INTRODUCTION (20 mins)

1. There is talk about "cybersecurity in healthcare" these days. When you hear the phrase, "cybersecurity in health care," what does it mean to you?

GO AROUND THE ROOM

2. Is cybersecurity a big issue for you in your own work at the healthcare organization or practice where you are principally employed? Why or why not?

PROBE IN SOME DETAIL

3. Do you think health care organizations like yours generally do enough to protect healthcare data or against attacks on their computer systems? Why or why not?

Here are some things we've heard said.

4. Most (doctors, organizations like yours, etc.) see the most common cyber threats as nuisances rather than dangers, since they think many don't succeed and most breaches involve relatively small amounts of health care information.

Would you agree or disagree, and why?

5. Most (doctors, organizations like yours, etc.) see a major cyberattack as potentially disastrous, but they think the likelihood is very low and their ability to avoid it is very limited.

Would you agree or disagree, and why?

6. How effective do you think staff training at your organization or practice is in preventing or reducing the impact of cyber-attacks?

7. Think about a warning beeper, buzzer, siren or alarm. If you were to imagine some problems a healthcare organization or practice might be alarmed about, think about how much it would beep or how loud the alarm might sound, from a little beeper for a little problem to a huge loud siren for a really dire problem. You can imagine flashing lights or any other form of alarm too, or act out the siren.

What would the beeper or alarm be like for each of these problems at your institution: **GET A FEW REACTIONS FOR EACH, ASK WHY THAT REACTION.**

- An infection control problem
- An electric blackout
- A jammed elevator
- A breach of health care data
- Several broken windows
- Failure of the organization's computer network

II. RESPONDENT ORGANIZATIONS (20 mins)

1. What's happening in cybersecurity, that is, protection of healthcare data and against computer attacks, at your organization?

2. How much return on investment do you think your organization or practice can get from its spending, if any, on cybersecurity?

3. How do you personally get information about cybersecurity?

PROBE FOR DETAILS

4. a. How familiar are you with HIPAA Security Risk Analysis?

   b. How often do you have them at your organization or practice, and have they helped it? Why or why not?

5. Do you know if your organization or practice has a portion of your budget allocated specifically for cybersecurity?

a. **IF YES:** Is the budget for cybersecurity at your institution about right, too much, or too little? And why do you say that?

6. Are there things you've had to neglect in order to have funds for cybersecurity? **IF YES:** What?

7. What would prompt your organization or practice to spend more on cyber security?

8. How often have you had attempted cyberattacks at your organization? Were any successful?

IF SUCCESSFUL, PROBE. (IF MORE THAN ONE, THE MOST RECENT)

- What happened?
- How long did it take to detect the problem?
- What were the consequences

III. ISSUE PERCEPTIONS (20 mins)

Now I'd like to find out about some cyber topics, based on your own perceptions and experience.
GET THE SENSE OF THE ROOM ON EACH, WITHOUT CALLING ON EVERYONE

1. What proportion of health care organizations or practices do you think have faced cybersecurity attacks in the past couple of years?

2. What kinds of people do you think are usually behind the cybersecurity threats at health care organizations or practices like yours?

3. What do you think the motivations of cyber-attackers most often are?

4. What do you think are the most common types of cyber threats health care facilities like yours face?

5. Some cyber-attacks involve "malware," or the insertion of harmful programs into computer systems. What do you think are the most frequent types of malware used in cyber-attacks against health care organizations or practices like yours?

6. When hackers break into health care computer systems at organizations or practices like yours, how do you think they usually get in?

7. Is there a clear set of rules or procedures that health care organizations or practices like yours should follow to maintain cyber security?

IV. FACT SHEET (20 mins)

DISTRIBUTE HANDOUTS WITH THE POINTS BELOW
Here is a fact sheet with the results of some research on cyber security by the consulting firm Accenture, Verizon, and the American Medical Association. Please read it through silently, and circle the numbers of the two items that seem most important or impactful to you. Then we'll discuss them

AFTER THEY FINISH READING AND CIRCLING, GO OVER EACH POINT, SEE HOW MANY CIRCLED IT AND WHY, AND WHY OTHERS DIDN'T CIRCLE IT.

Handout 1

Read silently and circle the two that are most important or impactful to you.

1. 83% of doctors say their health care facilities have experienced at least one cyber-attack.
2. 68% of the sources of successful cyber-attacks in health care are insiders working in the affected institution – the only industry for which this is the case.
3. The motive in two-thirds of breaches is financial, and one in four is done for fun. Grudges are responsible for 7%, espionage 3%.
4. Around three-fourths of breaches in health care are 1) misuse of access privileges, 2) theft, loss, or improper disposal of devices, especially mobile devices, and 3) delivery or publishing errors. The rest involve hacking, malware (malicious programs), or phishing (clicking on fake emails).
5. Over 70% of attacks involving malware install "ransomware," which locks computers unless a ransom is paid.
6. In half the cases where health care systems are breached by hackers, they use credentials stolen from or tricked out of legitimate users.
7. The Department of Health & Human Services is developing guidelines for health care facilities for cybersecurity

V. **MESSAGING (10 minutes)**

Here are some reasons people offer as to why health care organizations and practices should pay more attention to cyber security. Again, read them and circle the two that seem most important to you; no talking until everyone's done.

AFTER THEY FINISH READING AND CIRCLING, GO OVER EACH POINT, SEE HOW MANY CIRCLED IT AND WHY, AND WHY OTHERS DIDN'T CIRCLE IT.

Handout 2

1. Effective staff training reduces the likelihood of successful cyber-attacks by 40%.
2. Among doctors, 53% are worried that future cyber-attacks could damage patient care.
3. Health care organizations and practices that don't meet cybersecurity standards may face whopping big increases in insurance premiums.

4. At its peak, the "WannaCry" ransomware attack last year infected the computer systems at one-third of Britain's health care organizations, with particular impact on hospital emergency and accident departments.
5. Doctors and nurses may have training in cybersecurity added to their Continuing Medical Education requirements.
6. Hospitals, clinics, and other health care facilities failing to meet cybersecurity standards might lose their accreditation.
7. Financial incentives or subsidies could be given to health care organizations and institutions to upgrade their cyber security

VI. CYBERSECURITY INFORMATION AND HHS GUIDELINES (20 minutes)

1. What do you think is the best approach to learning about cybersecurity?

IF NOT MENTIONED, PROBE:
- Downloadable comprehensive documents
- Online learning applications or courses

As I mentioned, the Department of Health and Human Services is preparing guidelines for cybersecurity in health care.

2. What would you like to know about these guidelines?

3. What information would be most helpful to have in the guidelines?

4. What formats would be most useful to your organization or practice for information about the content of the guidelines?

IF NOT MENTIONED, PROBE:
- Checklists
- Pamphlets
- Posters for the workplace
- Short online videos

5. What is the best way for HHS to disseminate cyber security related guidance to relevant stakeholders?

IF NOT MENTIONED, PROBE:
- Email? (And from who – HHS? AMA or other professional association?)
- Direct mail (snail-mail)
- Website
- Pop-ups in health care computer systems when requests made the seem to break the guidelines
- Professional conferences
- Professional publications, blogs, and websites

- Health care trade union publications and blogs
- In CME courses (specifically on cybersecurity? Or inserted into other CME subjects?)

6. As you may know, this focus group is sponsored by the U.S. Department of Health & Human Services, who will be publishing the guidelines. Is there anything I haven't asked that you'd like to tell them?