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

SCREENER

Please fill this in before the group. If you don't know the answer to any of these questions, please indicate that.

1. Position

2. Organization and type

3. Devices used by your organization or practice that transmit patient information electronically:
Server desktop computer laptop tablet smartphone other (specify)

4. Cyber training – frequency, extent, who trains, who is trained

5. Person responsible for cyber security at your organization or practice:
you another staff member external vendor/contractor

6. Total size of cyber security team, if any, including leader

7. Percentage of your organization or practice's budget spent on cyber security, if you know it

8. Is there monitoring of devices used for compliance with cybersecurity policy

9. Please rate your current level of concern with each of potential risks to your patient data: (very low, low, medium, high, very high) in terms of their likelihood, impact on patient care, and cost to your organization

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0990-0379. The time required to complete this information collection is estimated to average ___30 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, to review and complete the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: U.S. Department of Health & Human Services, OS/OCIO/PRA, 200 Independence Ave., S.W., Suite 336-E, Washington D.C. 20201, Attention: PRA Reports Clearance Officer

Risk factor	Likelihood	Impact on patient care	Cost
a. Lost, stolen, or damaged devices containing patient information:			
b. Patient information is inappropriately accessed by current or former employee			
c. Environmental/natural disasters (fires, floods, etc.) that damage devices:			
d. Introduction of computer malware or virus caused by an employee clicking on a “phishing” email or email attachment			
e. External “ransomware” attack where patient data is held “hostage” until a ransom is paid:			

10. What percentage of the overall number of cyber security attacks that your organization has faced over the last year fall into each of the following five categories? (Responses should add to 100%)

    a. Lost, stolen, or damaged devices containing patient information:

    b. Patient information is inappropriately accessed by current or former employees:

    c. Environmental natural disasters (fires, floods, etc.) that damage devices:

    d. Introduction of computer malware or virus caused by an employee clicking on a “phishing” email or email attachment

    e. External “ransomware” attack where patient data is held “hostage” until a ransom is paid

11. How do you currently receive information and education related to cybersecurity from each of these sources? If so, how often? (always, sometimes, never)?

    a. Medical specialty or provider organization:

    b. Third-party vendors:

    c. Federal Government

    d. Via Internet searches:

e. Professional association and/or trade association

f. Other (please specify):

12. What communication, if any, do you receive from HHS at present? And do you read it?