Sentara Research Data Attestation Statement

Access to confidential healthcare data is essential for medical research. Access to Sentara's confidential healthcare data for research is regulated by Institutional Review Boards (IRB) and federal laws and regulations. Access to Sentara's confidential healthcare data is governed and managed by Sentara Healthcare acting as a covered entity, as defined by the HIPAA Privacy Rule. Use of Protected Health Information (PHI) is strictly regulated by the HIPAA Privacy Rule but use of de-identified data also requires strict confidentially to avoid any misuse, reuse, or reidentification of Sentara's healthcare data. In this document, confidential healthcare data refers to both PHI and de-identified data used for research.

Any individual granted access to confidential healthcare data has an obligation to know and understand the Sentara privacy and security policies and to follow those policies consistently. Breaches of data privacy or security can adversely affect the welfare of patients and the reputation of healthcare organizations involved in research. Failure to comply with Sentara privacy and security policies may result in disciplinary action including termination of data access, suspension of hospital privileges, and possible termination of employment or disciplinary action by affiliated organizations. Every individual with access to confidential healthcare data has a legal and ethical obligation to safeguard the data and must agree to the following terms and conditions.

1. I understand the importance of confidentiality and security when using confidential healthcare data for research and I understand that any deviation from the regulations and policies that govern access to Sentara's confidential healthcare data will have serious consequences.
2. I have completed the health privacy and human subjects research training modules offered through the Collaborative Institutional Training Institute (CITI). It is my obligation to keep my training up to date. I will also periodically review the information available through the Sentara Health Research Center's website and other resources regarding the responsible conduct of research and the proper use of confidential healthcare data, as defined by the HIPAA Privacy Rule.
3. I understand that I do not have any ownership rights to the confidential healthcare data that I gain access to or receive from Sentara.
4. I understand that I may only access confidential healthcare data when it is necessary, appropriate, and lawful to do so in the performance of my research. The confidential healthcare data may be used only for the approved purpose, as defined by an approved IRB protocol.
5. I understand that confidential healthcare data may not be accessed or used for personal reasons or any reason that does not directly pertain to the approved research project.
6. I understand that I cannot disclose, copy, or transmit any confidential healthcare data to any person who is not authorized to access the data by the IRB protocol and the Sentara data approval process.
7. I understand that confidential healthcare data stored at a Sentara facility in hard copy must be stored in locked drawers or cabinets.
8. I understand that computer workstations, laptops, and mobile devices with Sentara data must be locked when not in use and must utilize screen lock security.
9. Log-on credentials must be securely maintained and may not be shared, disclosed, or publicly posted.
10. I understand that I must log out of software or other applications that collect or maintain confidential healthcare data when I leave a workstation with Sentara data.
11. I understand that confidential healthcare data that I collect must be stored in a RedCap database or a whole-disk-encrypted and password-protected device.
12. I understand that CDs, USB flash drives, and other mobile storage may not be used to store any confidential healthcare data without written authorization from the Sentara Health Research Center, and if approved, these devices must utilize encryption and password protection.
13. I understand that Sentara may transfer confidential healthcare data to me by granting access to a password-protected secure file-transfer site and no confidential healthcare data should be transferred

by email.

14. I understand that confidential healthcare data in electronic form must be removed from my computer, laptop, or other electronic device at the time such device is retired or before the device can be transferred to another area or department. Electronic data must be cleared using software or hardware products that overwrite/delete the data. It is my responsibility to know whether the confidential healthcare data I received must be destroyed or returned to Sentara at the end of the research project.
15. I understand that upon termination of my employment or school enrollment, I will immediately return any confidential healthcare data and research data storage devices to Sentara.
16. I understand that if the provided confidential healthcare data is de-identified or a limited data set, I may not request PHI, or a link to PHI from Sentara or make any attempt to re-identify the information contained in the limited or deidentified confidential healthcare data or attempt to contact the individuals whose information may be contained in the confidential healthcare data, unless such contact is stipulated in the IRB-approved protocol.
17. I understand that I am responsible for notifying the Sentara Health Research Center and the Sentara Privacy Officer immediately if:
    a. My credentials used to access confidential healthcare data have, or may have been hacked, disclosed, or otherwise compromised.
    b. I know or suspect that the confidential healthcare data has been inappropriately accessed, used, disclosed, shared, hacked, or otherwise compromised.
    c. I have misplaced or otherwise lost possession of any documents, notebooks, devices (computer, laptop, mobile device, mobile storage) or other storage that contains confidential healthcare data.
    d. I overhear, discover, or become aware of any confidential healthcare data that is not being protected as set forth herein.
18. I understand that Sentara reserves the right to audit my work environment, computers, or other areas and devices that are used to access/use the confidential healthcare data to ensure compliance with the requirements outlined herein.
19. I understand that obligations of confidentiality continue indefinitely, even after termination or expiration of my employment, contract, or other relationship with Sentara and even if I no longer have the confidential healthcare data in my possession.
20. I understand that any non-compliance and/or request or instruction to ignore or bypass the requirements set forth in this document must be reported to Sentara immediately.
21. General questions about compliance with the terms should be directed to the Sentara Health Research Center or the Sentara Privacy Officer.

By signing below, I acknowledge that I have read and will abide by the Sentara Data Use Attestation Statement outlined here and that failure to abide by the terms of this statement will result in disciplinary action up to and including termination of employment or school enrollment.

_____ _____

Signature Date

_____

Print Name Office of Research ID #