EVMS Institutional Compliance
Data Use Requirements

Introduction/Background:

Personally identifiable Data("PID"), protected health information ("PHI"), or other sensitive information ("SI") (collectively, PID, PHI, and SI shall be known as the "Data") may be used by Centers, Departments, Project Leaders or Principal investigators (PI) to perform services or to conduct research that has been approved by EVMS. In order to provide this use, EVMS may enter into one or more agreements with the Data provider(s) that place responsibility on EVMS to ensure that the Data is kept confidential and accessed only in a manner permitted by the Data Provider. As such, every individual that will have access has a legal and ethical obligation to safeguard the Data as outlined herein.

Accessing and Using Data:

You may only access and use Data when it is necessary, appropriate, and lawful to do so in the performance of your duties at EVMS. This means that:

1) Data may only be used for the approved purpose (providing specific services requested by the Data provider or, in the case of research projects, for the project approved by the EVMS IRB and the Data Provider). Any deviations from such use must be specifically approved by the Data provider and/or the EVMS IRB (if applicable). Note that an approved IRB protocol does not automatically grant you the ability to search, access, identify, disclose, discuss, release or reuse Data for future projects, even if you have access to that Data for other purposes or you have been granted access to that Data in the past for another project.
2) Data may not be accessed or used for personal reasons (to check on someone you know, at the request of someone else, out of curiosity, etc.).
3) Data and/or access to Data may not be provided to any unauthorized person or entity (unauthorized means that the person or entity is not part of EVMS and/or does not have a need to access the Data or purposes of this project), without the express written permission of the Data provider. This also means that you may not share Data with a non-EVMS co-investigator, until/unless such use is approved by the Data Provider.

Protecting Data:

To keep Data from unauthorized access or use, it must be protected at all times by using the following measures.

Security:

1) Data in hard copy must be stored in locked drawers or cabinets.
2) Computer workstations, laptops, and mobile devices must be locked when not in use and must utilize screen security (alpha-numeric or fingerprint enabled).
3) You must log out of software or other applications that collect or maintain Data when you leave a workstation.
4) CDs, USB flash drives, and other mobile storage should not be used to store any PID, PHI, or SI without explicit permission and, if approved, they must utilize encryption/password

protection.

5) All EVMS workstations and laptops must be maintained in accordance with EVMS Network Information Center (NIC) standards, including but not limited to, up-to-date virus protection.
6) EVMS electronic systems may only be accessed with the credentials (User ID and password) assigned specifically to you by the NIC. Credentials may not be shared, disclosed, or publicly posted and you will be held responsible for any unauthorized access that results if your credentials are shared.
7) You may not use any cloud services for Data unless approved by the NIC.
8) EVMS network accounts (ending in "@evms.edu" or "@CONRAD.org") must be used for all communications. Further, emails with Data may not be manually or automatically forwarded to a non-EVMS personal email service (Gmail, yahoo, AOL, etc.) and you may not use any "pop" protocol to force your EVMS account email into a non-EVMS personal account.
9) You may not use any tool or techniques to break, exploit, or otherwise circumvent established security measures.
10) All Data in electronic form must be removed from your computer, laptop, or other electronic device at the time such device is retired and/or before the device can be transferred to another area or department.
11) Data and/or devices containing Data may never be thrown in standard trash bins. Data in hard copy must be destroyed by shredding or other method that renders the Data unreadable and unable to be reconstructed. Electronic Data must be cleared using software or hardware products that overwrite/delete the data. It is your responsibility to know whether the Data you receive must be destroyed or returned to the Data provider at the end of the services or research project.

Privacy:

1) Data must be kept in strict confidence regardless of whether it is communicated to you in hard copy, faxed, electronically transmitted, via oral conversations, or in printed or other formats. This confidence must be kept when performing your duties, as well as during breaks, rest periods, and time away from EVMS.
2) You are responsible for ensuring that discussions concerning Data do not occur in hallways, elevators, or other public areas where someone not authorized to receive the Data could inadvertently overhear PID, PHI, or SI.
3) You may not share, release, or broadcast Data in any manner, including posting of PID, PHI, or SI on any list service, or professional or social media site.
4) If the Data provided is de-identified or a limited data set, you may not request PHI, or a link to PHI, from the Data provider or make any attempt to identify the information contained in the Data or contact the individuals whose information may be contained in the Data.
5) Upon termination of your employment, expiration of your contract or other termination of your relationship with EVMS, you will immediately return any confidential information to EVMS.

Compliance:

1) You are responsible for notifying the Center Director, Project Leader or PI , as applicable, and the EVMS Privacy Officer (wileyjp@evms.edu, 446-6008) immediately if:

a) Your credentials used to access Data have, or may have been hacked, disclosed, or otherwise compromised;
b) You know or suspect that the Data has been inappropriately accessed, disclosed, shared, hacked or otherwise compromised;
c) You misplace or otherwise lose possession of any notebook, device (computer, laptop, mobile device, mobile storage) that contains Data;
d) You overhear, discover, or become aware of any Data that is not being protected as set forth herein.

2) EVMS reserves the right to audit your work environment, computers, or other areas and devices that are used to access/use the Data in order to ensure compliance with the requirements outlined herein.
3) Obligations to confidentiality continue indefinitely, even after termination or expiration of your employment, contract, or other relationship with EVMS and even if you no longer have the Data in your possession.
4) Any non-compliance and/or request or instruction to ignore or bypass the requirements set forth in this document must be reported to EVMS OGC/Institutional Compliance at 446-7250, OGC@evms.edu immediately.
5) General questions about compliance with the terms should be directed to the EVMS Office of the General Counsel/ Institutional Compliance Office, 446-7250, OGC@evms.edu.

By signing below, I acknowledge that I have read and will abide by the Data Use Requirements outlined and that failure to abide by same, will result in disciplinary action up to and including termination.

_____ _____

Signature Date

_____

Print Name