Yale School of Public Health (YSPH) Data Security

At the request of the Dean of YSPH, the Yale Health Insurance Portability and Accountability Act (HIPAA) Privacy Office and Office of the General Counsel reassessed the University’s designation of its HIPAA Covered Entity. As a result of this review, the Yale Covered Entity was redefined to exclude YSPH. This change will make your YSPH work easier in some respects, but it does not change your obligation to protect the security of sensitive and confidential information. Because the failure to protect the confidentiality, integrity, and availability of your data could harm research subjects, embarrass the University, damage YSPH’s relationship with the government and collaborators, and violate contractual obligations, you must meet the requirements set out below for the security of “Sensitive Information” and “Other Confidential Information.”

**Sensitive Information** includes (i) data that would customarily be shared only with a person’s family, doctor, lawyer, or accountant (for example, sensitive or potentially stigmatizing health information); (ii) data that could be exploited for criminal or other wrongful purposes (for example, Social Security numbers); or (iii) data that Yale is contractually obligated to keep confidential (for example, data that is subject to a non-disclosure agreement).

**Other Confidential Information** includes (i) health information that is neither sensitive nor potentially embarrassing; (ii) students’ education records; (iii) Yale personnel information, or (iv) data that Yale is contractually obligated to keep confidential (for example, data that is subject to a non-disclosure agreement).

Additional examples of Sensitive and Other Confidential Information are set out below.

The following are other important implications of the decision to exclude YSPH from the definition of Yale’s covered entity:

- Within YSPH, there is no need for a HIPAA research authorization or waiver determination or for completing HIPAA training prior to approval of a research protocol. However, if you are involved in a Yale School of Medicine study using Personal Health Information provided by YSM, you will be required to complete HIPAA training prior to receiving the YSM data. In this respect, you are no different than YSM’s non-Yale collaborators.

- If your proposed research will be limited to YSPH but involves obtaining data from a covered entity (including YSM), the entity providing the data source will be required to ensure that your access to the data is permitted by HIPAA. In such a case, the entity’s IRB may be asked to facilitate the release of the data by granting a waiver of authorization as a Privacy Board. If you are collaborating with YSM or YNHH, the Yale IRB will make this determination.
Your Obligations Going Forward

OBLIGATION 1:  **Determine whether your data may be covered by HIPAA.**

Despite the change in YSPH’s status, your data may be covered by HIPAA if you are not using it for research but instead are using the data to help treat patients, obtain payment for treatment, or support the operational work of a covered entity (http://hipaa.yale.edu/guidance/index.html). (If you have obtained data for one of these purposes or using data obtained for one of these purposes, you may be asked to sign a “Business Associate Agreement” with the person or entity providing the data.) If you believe that you may have data covered by HIPAA, you must contact the Deputy HIPAA Privacy Office for the School of Medicine at angela.oren@yale.edu / (203) 737-1781.

OBLIGATION 2:  **Identify Your Sensitive Information. You must identify all information under your control in the following categories.**

**Category 1:**
(i)  Information that identifies a person  (This includes for example, name, telephone number, fax number, street address, e-mail address, biometric identifiers, or photograph.)

in combination with:

(ii)  Sensitive or potentially embarrassing health information. This includes, for example, information about genetic testing, HIV status, sexually transmitted diseases, substance abuse, mental illness, life-threatening illness, fertility issues, or sexual issues. When deciding whether information is sensitive or potentially embarrassing, err on the side of being over-inclusive, not under-inclusive.

**Category 2:**
(i)  Information that identifies a person. (This includes for example, name, telephone number, fax number, street address, e-mail address, biometric identifiers, or photograph.)

in combination with:

(ii)  Social Security number, medical record number, health insurance number, bank account number, credit card number, driver’s license number, or passport number.
Category 3: Information covered by a non-disclosure agreement, a confidentiality agreement, or other contract that requires you to protect the information of another party. (Depending on the security requirements imposed by the contract, data in this Category may be considered “Other Confidential Information.”)

OBLIGATION 3: Identify Other Confidential Information. You must identify all information under your control in the following categories.

Category 1: Information that identifies a person. (This includes for example, name, telephone number, fax number, street address, e-mail address, biometric identifiers, or photograph.)

in combination with:

(ii) Health information that is neither sensitive nor potentially embarrassing.

Category 2: The education records of students.

Category 3: Information about Yale faculty or staff performance, discipline, or evaluations.

Category 4: Information covered by a non-disclosure agreement, a confidentiality agreement, or other contract that requires you to protect the information of another party. (Depending on the security requirements imposed by the contract, data in this Category may be considered “Sensitive Information.”)

OBLIGATION 4: Implement Appropriate Data Security Measures.

If you have Sensitive or Other Confidential Information, you must ask the YSPH Desktop Support Provider to review your existing equipment, applications, and security measures and to recommend and implement any upgrades, updates, or additional security measures (contact 203-432-9000, 203-785-3200, or e-mail helpdesk@yale.edu). The Support Provider will apply the Minimum Security Standards for YSPH Computer Equipment and Applications (Appendix A). If you do not agree that a recommended upgrade, update, or security measure is necessary, you may ask the Chief Information Security Officer to review the Support Provider’s recommendation.

A Security Incident is any event that leads you to believe that Sensitive Information or Other Confidential Information has been lost, stolen, improperly disclosed, improperly accessed, or damaged. If you believe a Security Incident has occurred, you must report it immediately to Yale Information Security at 203-436-5872 or ciso@yale.edu
APPENDIX A: MINIMUM SECURITY STANDARDS FOR YSPH COMPUTER EQUIPMENT AND APPLICATIONS

**Passwords:** Passwords must be used and must meet ITS strength requirements, with no automatic logon. (See: [http://its.yale.edu/how-to/create-strong-password](http://its.yale.edu/how-to/create-strong-password)) Passwords may not be shared.

**Hardware Capabilities:** Devices must be capable of supporting up-to-date security software and other minimum security requirements and must be listed by the manufacturer as devices for which support is still available.

**Central Management:** Devices must be subject to ITS central management.

**Anti-Malware Software:** Active, up-to-date, and centrally managed anti-malware software must be installed on all devices.

**Administrative Access:** When a user requires administrative access, a separate administrative account must be created for administrative tasks, and

- all day-to-day work must be performed in a user account without administrative privileges;
- user administrative accounts must only be used for system maintenance, application installation, and similar tasks; and
- Whenever possible, user administrative accounts must be denied local logon privileges to prevent abuse or accidental use.

**Private IP Addresses:** Devices that are wired to the Yale network must use private IP addresses, except for devices hosting websites that must be accessed by persons outside of Yale.

**Encryption:** All laptops, mobile devices, and workstations storing Sensitive Information or Other Confidential Information must be encrypted.

**Physical Security:** All laptops and all workstations storing Sensitive Information or Other Confidential Information must be secured when not in the possession of the user. Servers must be housed in data centers or server rooms with electronic access controls (such as badge readers) and alarms. Acceptable methods of ensuring physical security include storage in a locked office or locked drawer and the use of locking cables.

**Remote Access:** Remote access to devices on the Yale network must be accomplished through the Yale VPN connection. ([http://its.yale.edu/services/wifi-and-networks/vpn-campus-access](http://its.yale.edu/services/wifi-and-networks/vpn-campus-access))
Remote ("Cloud") Storage: Yale data may be stored or shared remotely only through a Yale-approved remote storage vendor.

Web Servers: Web servers may provide web services only and may not be used to store data.

Wireless Access: The “Yale Secure” Wireless network must be used for wireless Internet access.

Secure Disposal: All Sensitive Information and Confidential Information must be securely deleted before a device may be transferred to a new user. Devices that can no longer be used must be securely destroyed.