Data Privacy - Quick Reference

Data Privacy

This quick reference provides guidance and resources to protect restricted personally identifiable information following UC information privacy policies and PHI/HIPAA guidelines.

About Information Privacy at UC

- The University of California is committed to high standards of excellence for protection of information assets and information technology resources that support the University enterprise.
- The University processes, stores, and transmits an immense quantity of electronic information to conduct its academic and business functions.
- Without the implementation of appropriate controls and security measures, these assets are subject to potential damage or compromise to confidentiality or privacy, and the activities of the University are subject to interruption.
- Details on information privacy is available in the Electronic Information Security Bulletin

UCSF Employee Responsibility

- Every UCSF employee and student is required to read and sign the Confidentiality Agreement.
- **It is your individual responsibility to not violate the agreement.**

Requirements for Processing PHI/HIPAA Information in BearBuy

- The Health Insurance Portability and Accountability Act (HIPAA) was passed to protect the confidential medical and billing records of our patients.
- Under HIPAA, Protected Health Information (PHI) is individually identifiable health information which is created in the process of caring for the patient, and is transmitted or maintained in an electronic, written, or oral manner.
  - If you need to view, use, or share this type of information, you will need to follow information privacy guidance and policies.
- If a supplier may potentially have access or exposure to PHI, you must ensure the BearBuy transaction is **flagged as HIPAA**.
- The supplier also needs to sign a Business Associate Agreement (BAA).
  - Please contact your department's assigned Campus Procurement Buyer to assist the supplier in signing the BAA.

How to Handle Data Privacy in BearBuy

- PHI and sensitive or private information should not be entered into BearBuy unless absolutely necessary.
- Only attach or enter information that is necessary to complete and process a BearBuy transaction.
  - Include this information only if your transaction will not be processed without such information.
- When attaching documents in BearBuy, attach only the required pages in a document.
- If necessary, properly redact PHI and sensitive or private information from attachments.
  - Remove the Social Security Number when the vendor ID is on the document.
  - Ensure the information is not decipherable in any way. For example, using a Sharpie to redact is insufficient because you can often read right through it.
- Use software such as Adobe Acrobat to redact information.
  - Contact your department manager or the ITS Service Desk for guidance.
- Make sure you remove your extra electronic and paper copies when done.

Remove ALL 7 Supplier or Payee Data Elements to De-identify Data

- **TIP: Do not attach W-9 forms to BearBuy orders.**

1. Social Security numbers
2. Home Address (unless the same as the business address)
3. Home Phone Numbers (unless the same as the business phone number)
4. Driver's license or California Identification Card number
5. Financial, credit card, or debit card account numbers, as well as security codes, access codes, or passwords
6. Health insurance information
7. Passport

Remove ALL 18 PHI Elements to De-identify Data for PHI/HIPAA

- If you have information that is considered PHI, de-identify the data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members.

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all

elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

Additional Resources:

- The Privacy Website: http://hipaa.ucsf.edu/default.html
- The Privacy and Confidentiality Handbook: A great resource with an overview of privacy, including FAQs, and the Confidentiality Statement http://hipaa.ucsf.edu/Privacy%20Handbook.pdf
- The UCSF Confidentiality Statement: http://hipaa.ucsf.edu/education/downloads/ConfidentialityStatement.pdf
- HIPAA 101: Basic privacy training that every employee should receive upon hire http://hipaa.ucsf.edu/education/downloads/HIPAA101Training.pdf
- An explanation of PHI and a list of the 18 identifiers: http://www.research.ucsf.edu/chr/HIPAA/chrHIPAAphi.asp
- From the US Department of Health & Human Services, an explanation of the Minimum Necessary Standard: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.pdf
- UCOP Electronic Information Security: http://policy.ucop.edu/doc/7000543/BFB-IS-3
- Legal requirements on Privacy of and Access to Information: http://policy.ucop.edu/doc/7020463
- UCSF Information Security and Confidentiality: http://policies.ucsf.edu/650/65016.htm