Mailman IT Data Security Advisory: Defining De-Identified Data, 11-30-11

I thought it would be helpful to circulate the official Privacy Rule guidelines for "de-identified data" as it pertains to protected health information. There seem to be many differing opinions on the subject at the School, and the requirements are more stringent than many of you may be aware.

Full details can be found here: http://privacyruleandresearch.nih.gov/pr_08.asp and are also linked to from the IT section of our Mailman Web site. **In a nutshell:** According to NIH: "…The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members…"

These data include:

1. Names

2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are 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. Telephone numbers

5. Facsimile 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 fingerprints and voiceprints

17. Full-face photographic images and any comparable images

18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification

If you have questions or concerns about this, or any other data security issue, please don't hesitate to call. Thank you.

Elizabeth Tashiro
(212) 342-3021
Ass't. Dean of Information Technology
Mailman School Of Public Health, Columbia University