Mailman Data Security Advisory, 10-10-11

Dear Faculty and Staff,

As you know, protecting our own private data and the data of those we serve is an increasing priority in this information age. To this end, I want to make you aware of the current IT-specific University policies related to securing private data, who they cover, and some of the tools and services we provide to enable your compliance. In addition, I want to encourage you to attend School Assembly tomorrow (Oct 11) where the head of CUMC Network Security, Soumitra Sengupta, will do a data security presentation and Q&A. We have also created an area on the Mailman Website where we've aggregated the latest University policy information http://www.mailman.columbia.edu/faculty-staff/administrative-offices/information-technolgy-online-resources/it-guidelines-policies. You can also access the CU Administrative Policy Library Computing & Technology section for updates; policies are being updated on an ongoing basis: http://policylibrary.columbia.edu/node_browser/nodes_by_category/term/34

Do these policies apply to me?
- These policies apply to all faculty, staff, students and affiliated groups working on behalf of the University.

What data is considered private?
- This user-friendly data classification table lists what data you need to protect:
http://www.columbia.edu/cu/administration/policylibrary/policies/00bb9c67198088230119b4fac83a0003/8.2_-_Data_Classification_Policy_appendix_B_-_final_1209922354756.pdf

What am I required to do to keep private data secure?
http://www.columbia.edu/cu/administration/policylibrary/policies/00bb9c67198088230119b4fac83a0003/8.1_-_Data_Classification_Policy_appendix_A_-_final_1209922341420.pdf
Are there penalties associated with a private data leak?
- Yes. The government has been levying ever-increasing monetary fines against the institutions in which the breach occurs. A leak of 10,000 records now costs upwards of $2M. The University is working to determine who will be responsible for the fine under the policy. Suffice it to say, a fine of this size against a specific school or department could be catastrophic, and must be avoided.

What tools and services are available to help me comply?
- Hard disk encryption, secure disposal of old data storage devices, secure file storage, are just a few. Please contact me or another member of Mailman IT for details.

What do I do if I suspect a leak of sensitive data?
Please e-mail security@columbia.edu immediately for support, cc: Elizabeth Tashiro at es2222@columbia.edu

Are there any resources currently available that give an overview of the issues?
- CUMC Privacy Officer Karen Pagliaro-Meyer and Security Officer Soumitra Sengupta prepared this presentation incorporating the most recent governmental policy changes in HITECH. While parts of it emphasize patient care concerns that may be less relevant to those faculty and staff who do not deal with patients, the overall issues of data privacy and the ramifications of a breach are well documented and relevant to all. I encourage you to take some time to view this presentation at your earliest convenience.
http://a2learning.cumc.columbia.edu:8080/ess/echo/presentation/367f4ef2-5b4e-4b5e-a48b-c9b24b18b21c

What if I have additional questions or concerns?
Please always feel free to reach out to CUMC's HIPAA Office, the Office of IT Security (urls below) or my office.

http://www.cumc.columbia.edu/hipaa
https://secure.cumc.columbia.edu/cumcit/secure/security/index.html

Thank you.

Elizabeth Sparrow Tashiro
Asst. Dean of Information Technology
Mailman School of Public Health
Tel. (212) 342-3021