From:	UMMS Communications
To:	UMASSMED; UMassWorc Dept Heads; UMassWorc Dept Heads Information; AAG; Faculty List UMMS
Subject:	Compliance with data security and breach notification laws
Date:	Thursday, June 06, 2013 11:27:07 AM

TO: Members of the University of Massachusetts Medical School Community

FROM: Robert E. Jenal, Executive Vice Chancellor, Administration & Finance

DATE: June 6, 2013

SUBJECT: Compliance with data security and breach notification laws

A critical issue facing UMMS is compliance with data privacy and breach notification laws, including the Health Insurance Portability and Accountability Act (HIPAA). The UMMS community routinely engages in academic and research activities requiring regular access to information protected by a number of federal and state legal requirements, such as HIPAA, Mass. Gen. Laws Chapter 93H, and the Family Educational Rights and Privacy Act (FERPA). These and other laws require UMMS to take steps to protect its research or data subjects, staff and students by implementing controls over the use and disclosure of this information. Additionally, many entities with whom UMMS regularly collaborates establish contractual standards for how such data must be handled in academic, research, and administrative settings.

Further, the Office for Civil Rights of the U.S. Department of Health and Human Services recently revised the HIPAA regulations by, among other things, expanding the definition of "business associates." When UMMS creates, receives, maintains, or transmits protected health information on behalf of a covered entity as a result of some agreement or contract or through research activities, UMMS may be considered a "business associate." As such, UMMS may now be directly obligated to comply with many HIPAA requirements and significant civil and criminal penalties may be imposed for violations of these requirements.

To support UMMS's commitment to compliance in all aspects of campus operations and activities, UMMS's Office of Administration and Finance has worked with

Commonwealth Medicine's Office of Compliance and Review (OCR) to make resources available to UMMS faculty and staff on issues related to compliance with federal and state data privacy and breach notification laws and regulations, including HIPAA; and also to assist UMMS departments in analyzing whether they are "business associates" and thus, subject to the particular requirements that flow from that status. Faculty and staff are directed to contact OCR for education, training, monitoring, and consultation support concerning all of these matters. Such inquiries to OCR shall be copied to James G. Healy, JD, Associate Vice Chancellor for Management at James.Healy@umassmed.edu.

Contacting OCR:

Intranet Website**:** http://inside.umassmed.edu/commed/departments/ocr/index.aspx
Email: Compliance@umassmed.edu
Compliance contact number: (508) 856-6547

Please note that inquiries concerning **information security** issues should continue to be directed to Information Services at http://inside.umassmed.edu/is/index.aspx