WILLIAMS MULLEN
Where Every Client is a Partner®

July 2010

Health Care Law

Alert

Understanding HIPAA: Including Print and Copy Machines in Your Business's Compliance Plan

BY ANNE C. FOSTER, Certified Information Privacy Professional, MICHAEL E. BURKE, and MALCOLM E. RITSCH, JR.

Anne C. Foster

As one managed health care plan recently learned, overlooking copy and print machines when implementing HIPAA privacy and security measures is a costly mistake. On April 5, 2010, Affinity Health Plan of New York notified three state agencies, federal authorities, and more than 409,000 individuals of a breach of protected health information under the Health Insurance and Portability Accountability Act ("HIPAA").

Given that health care entities exercise great caution and go to great expense to ensure HIPAA compliance, how could an oversight of this magnitude occur? The answer is simple: like many of its peers, Affinity lacked the technical knowledge that its copy and print machines contained hard drives with the capacity to store protected health information. For purposes of HIPAA compliance, however, this technical knowledge is of vital importance to covered entities and their business associates. As one analyst recently estimated, nearly 80 percent (and potentially more) of all copy machines that businesses use contain at least one hard drive.

In the process of faxing, printing, scanning, and emailing, copy and print machines frequently retain information in a manner and format similar to a data storage device within a computer. Consequently, when a HIPAA-covered entity or its business associate returns the machine to a lessor, or otherwise disposes of the product, the entity may run the risk of a breach of protected health information.

Businesses can minimize this risk by encrypting or thoroughly scrubbing the data contained on the hard drive, or alternatively, by shredding the discs containing the data upon the machine's disposal. Also, businesses should note that connecting printers to an internet-accessible network may leave them (and the information they contain) vulnerable to a security attack. When performing a risk assessment, therefore, businesses should evaluate the likelihood of an outside security breach, considering whether an intruder could access protected health information or other confidential information stored on printer hard drives. If the likelihood of an outside intrusion is high, the business should regularly monitor its network for security attacks.

In addition to both the cost of providing notice to affected individuals and the cost of managing public relations following a breach, businesses that possess protected health information face greater penalties under the HITECH Act. Effective as of this past February, HITECH imposes stiff penalties on those entities that fail to abide by HIPAA

Williams Mullen
Health Care Law Alert.

Editorial inquiries should be directed to Wyatt S. Beazley, 804.420.6497 or wbeazley@williamsmullen.com,

rules. For example, before the passage of HITECH, the Secretary of Health and Human Services could impose only a $100 per day fine, up to a maximum of $25,000 per calendar year, for HIPAA violations. Pursuant to HITECH, the Secretary may now impose penalties ranging from $100 to $50,000 for the lowest category of violation. For the highest category of violation, the Secretary may seek penalties ranging from $25,000 to $1.5 million in a single calendar year.

Besides protecting sensitive health information, various federal and state statutes and regulations require protection of other types of sensitive personal information and impose significant penalties and disclosure obligations if the integrity of such information is compromised. Collectors and holders of sensitive personal information must take steps to protect such information from inadvertent disclosure pursuant to the regulations issued under the Gramm-Leach-Bliley Act; application of Section 5 of the Federal Trade Commission Act; standards issued by the Payment Card Industry; and laws in California, Massachusetts, and other jurisdictions. Also, companies that do not protect such personal information are at risk for private litigation and significant reputational damage, as well as the costs of remedying any deficiency in their information security systems.

For more information aout this topic, please contact the authors or any member of the Williams Mullen Health Care Team.

Health Care Law Team

Wyatt S. Beazley, IV
804.420.6497
wbeazley@williamsmullen.com

Michael E. Burke
202.293.8137
mburke@williamsmullen.com

James M. Burns
202.327.5087
jmburns@williamsmullen.com

Patrick C. Devine, Jr.
757.629.0614
pdevine@williamsmullen.com

Arlene J. Diosegy
919.981.4096
adiosegy@williamsmullen.com

Martin A. Donlan, Jr.
804.420.6934
mdonlan@williamsmullen.com

Anne C. Foster
804.420.6450
acfoster@williamsmullen.com

Jessica S. Jones
804.420.6493
jjones@williamsmullen.com

Travis G. Hill
804.420.6437
thill@williamsmullen.com

Samuel M. Kroll
757.473.5328
skroll@williamsmullen.com

Derek W.H. Kung
804.420.6587
dkung@williamsmullen.com

Courtney A. Miller
757.629.0665
cmiller@williamsmullen.com

Antonia A. Peters
919.282.1905
apeters@williamsmullen.com

Malcolm "Dick" E. Ritsch, Jr.
804.420.6486
dritsch@williamsmullen.com

WILLIAMS MULLEN
Where Every Client is a Partner®