THE NEW YORK STATE
Physician's HIPAA Privacy Manual
2nd Edition

William P. Keefer, Esq.
Lisa McDougall, Esq.

Sponsored by the New York State Bar Association's Health Law Section

New York State Bar Association publications are intended to provide current and accurate information to help attorneys maintain their professional competence. Publications are distributed with the understanding that NYSBA does not render any legal, accounting or other professional service. Attorneys using publications or orally conveyed information in dealing with a specific client's or their own legal matters should also research original sources of authority.

We consider the publication of any NYSBA practice book as the beginning of a dialogue with our readers. Periodic updates to this book will give us the opportunity to incorporate your suggestions regarding additions or corrections. Please send your comments to:
Publications Director, New York State Bar Association, One Elk Street, Albany, NY 12207.

ISBN: 978-1-57969-471-5
Product Number: 41196

FOREWORD

With the advent of the Health Information Technology for Economic and Clinical Health (HITECH) Act and proliferating regulations, the HIPAA landscape is becoming ever more complex. Navigating it successfully poses daunting challenges for health care providers and their counsel alike. This makes the need for guidance and direction all the more compelling. Since the privacy regulations took effect more than a decade ago, the Office of Civil Rights (OCR) has received an increasing number of complaints, with the majority of the complaints involving private health care practices. In some instances, significant penalties have been imposed and multi-million dollar settlements reached. While these have typically involved the theft of unencrypted electronic media, such as laptops or flash drives, penalties may also be imposed for inadvertent disclosure of protected health information (PHI) in an office setting or failure to have a Business Associate Agreement in place.

Against this backdrop, the Health Law Section, which has long functioned as a setting in which health care policy information may be exchanged, is proud to sponsor *The New York State Physicians' HIPAA Privacy Manual, 2nd Edition*. As with the previous edition, the objective is to simply, and thereby clarify, compliance with this intimidating array of policies and regulations. To that end, the Health Law Section has once again teamed with the Association to co-sponsor the *HIPAA Privacy Manual*, an invaluable resource that not only contains the necessary forms and authorizations for disclosure of PHI, but also provides a straightforward explanation of the applicable HIPAA and HITECH requirements, and how, when and to whom PHI may be disclosed. As such, the *HIPAA Privacy Manual* continues to be the manual that no health care organization or its counsel should be without.

Kenneth R. Larywon, Esq.

Chair, Health Law Section

New York State Bar Association

ACKNOWLEDGEMENT

The authors would like to acknowledge and thank others for their assistance in the process of putting together this manual—the law clerks at the New York State Bar Association, Kathryn Calista, Senior Attorney, Publications at the New York State Bar Association, and the Phillips Lytle Summer Associates of 2015. A special expression of gratitude is owed to Christopher R. Viney, Esq., one of the two original co-authors, and without whose help there would have been no manual to update.

ABOUT THE AUTHORS

WILLIAM P. KEEFER, ESQ.

William P. Keefer, a partner with Phillips Lytle LLP, graduated *magna cum laude* from St. Bonaventure University in 1985. He became a Certified Public Accountant in 1987, and graduated with honors from The George Washington University School of Law in 1991. He was admitted to practice in New York State and Massachusetts in January 1992. Since 2005, Mr. Keefer has devoted his practice to health law, and is the practice team leader of Phillips Lytle LLP's health law practice. Mr. Keefer represents physicians and physician groups, hospitals, nursing homes, and various other not-for-profit organizations that deliver health care services. He regularly counsels clients on fraud and abuse, privacy, reimbursement and other state and federal regulatory matters. Mr. Keefer frequently speaks and writes about health law issues. He is currently the Chair of the Bar Association of Erie County Health Care Law Committee. He is also a member of several not-for-profit boards of directors, and is a member of the Health Care Law Section of the New York State Bar Association and the American Health Lawyers Association.

LISA MCDOUGALL, ESQ.

Lisa McDougall, a *cum laude* graduate of the State University of New York at Buffalo, is of counsel to Phillips Lytle LLP. She received her J.D. degree from State University of New York at Buffalo Law School, and she is a former confidential law clerk to the Honorable Michael A. Telesca, U.S. District Court Judge, Western District of New York. Ms. McDougall has been practicing health care law for over twenty years and has represented a wide variety of clients including hospitals, physicians, nursing homes, various not-for-profit organizations, including not-for-profits with a mental health focus and health care consumers. She has defended numerous health care providers in matters involving local, state and federal regulators. She has counseled clients on issues including HIPAA, fraud and abuse, privacy, compliance and reimbursement and advance directives. Ms. McDougall frequently speaks and writes about a wide range of health care issues. She is the former chair of the Health Care Law Committee of the Erie County Bar Association, the former co-chair of the Women Physicians and

Women Attorneys' Task Force, a member of the Health Care Law and Elder Law Sections of the New York State Bar Association, and a member of the American Health Lawyers Association.

PREFACE

The New York State Physician's HIPAA Privacy Manual, 2nd Edition, continues to be a "hands on" tool for health care providers as well as their legal counsel. Updated to incorporate the changes required by the Health Information Technology for Economic and Clinical Health ("HITECH") Act and the most recent regulations, the new version contains 37 Policies and Procedures as well as the forms necessary to implement those policies and procedures. Changes of particular note include Breach Notification and new rules that directly require compliance from Business Associates. The *Manual* provides the day-to-day guidance necessary to allow the physician's office to respond to routine, everyday inquiries about protected health information, as well as the framework to enable the Privacy Officer and health care provider's counsel to properly respond to even non-routine issues. The *Manual* is organized in a way that parallels the various aspects of the HIPAA Privacy Rule—covering areas that include General Policies, Uses and Disclosures of Medical Information Without Patient Authorization, Operational Issues and Patient Rights. Importantly, the *Manual* incorporates pertinent New York State law considerations because HIPAA will defer to New York State law if there is a conflict and if New York State law is "more stringent."

For example, state law would be "more stringent" if the state law offers greater privacy protection of health information than HIPAA. Another example of a state law that is "more stringent" than HIPAA is a law that allows the patient or the patient's personal representative greater rights in accessing or amending the medical records. With the HIPAA preemption framework in mind, we authored *The New York State Physician's HIPAA Privacy Manual*, tailoring policies and procedures to reflect New York State law over HIPAA if the New York State law was contrary and more stringent.

Most health care providers will be considered "covered entities" by HIPAA and will accordingly need to perform a delicate balancing act. On the one hand, the provider may be tempted to stake out a position that it simply will not release protected health information until absolutely forced to do so. This contravenes one important tenet of HIPAA, which is that patients and their representatives generally have a right to access and control disclosure of protected health information. On the other hand, the provider

may take the position that as long as there is an authorization or a subpoena, the protected health information will be released. Again, this approach is not HIPAA-compliant and may also run afoul of New York State medical privacy laws. The area of medical record privacy is nuanced, and a broad brush approach does not work. Any question involving disclosure of medical records must be answered by a careful analysis of the facts, informed by knowledge of pertinent state and federal law. This *Manual* will help perform such a guided analysis.

As of the time of publication, the Office for Civil Rights ("OCR") had received and initiated reviews of more than 108,000 complaints about HIPAA since the privacy regulations took effect in 2003. The common complaints are that personal medical details were wrongly revealed, information was poorly protected, more details were disclosed than necessary, proper authorization was not obtained or patients were frustrated in getting their own records. Complaints are most often filed against the following types of covered entities: (1) private health care practices; (2) general hospitals; (3) outpatient facilities; (4) group health plans; (5) pharmacies and (6) insurers. Fines of $100 to $50,000 for each civil violation may be imposed. In 2014, there were nine settlements that totaled more than $10 million dollars. When this *Manual* was first published in 2007, there were none. The OCR also refers possible criminal violations to the Justice Department ("DOJ"), which could seek penalties of up to $250,000 in fines and 10 years in jail. As of this writing, the OCR made over 369 such referrals to the DOJ. Even though enforcement efforts are becoming more strict, by having compliant privacy policies and procedures in place, health care providers and their legal counsel will be able to better manage protected health information to minimize chances of running afoul of regulations.

The Office of _____, M.D.
HIPAA Privacy Policies and Procedures

Table of Contents

General Policies

Uses and Disclosures of Medical Information Without Patient Authorization