AHLA

How Does This Work?

Using Mobile Health Technology While Protecting Your Privacy

This guidebook can be downloaded for free at www.healthlawyers.org/PublicInterest

American Health Lawyers Association
1620 Eye Street, NW, 6th Floor
Washington, DC 20006
(202) 833-1100
www.healthlawyers.org

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

—From a declaration of the American Bar Association

Table of Contents

What is Mobile Health Technology?

Mobile health technology, commonly referred to as "mHealth," is the use of wireless mobile communication devices—such as smart phones, tablets, and "wearables" (e.g., Fitbit®)—to assist and/or improve the delivery of health care services; enhance communication between the patient and health care provider; help an individual track and/or achieve a personal health goal; or all of the above.

Consumers can now choose from a vast array of wearables and mHealth applications or "apps," which can be instantly downloaded to their smartphones or tablets for free or minimal cost. In September 2015, an IMS Institute for Healthcare Informatics (IMS) report revealed that the number of mobile health apps available to consumers now surpasses 165,000, nearly two-thirds of which are focused on general wellness such as fitness, lifestyle, stress, and diet. The remaining one-third are health apps that address specific health conditions, including many that are dedicated to women's health and pregnancy issues and apps that provide medication information and reminders. Mental health apps led among disease-specific apps, followed by apps for diabetic patients.[1]

mHealth technology is especially powerful because mHealth "tools," such as fitness apps, can continuously and instantly record, store, share, and/or analyze your health and wellness information by using an item of "consumer-grade hardware" that you already own (e.g., your

smart phone or tablet). The ability to track your personal health goals or share your medical information with health care providers through the convenience of something you already use on a daily basis (e.g., to check email, make phone calls, watch videos, take photos, obtain GPS directions, read restaurant reviews, and text family and friends) has great potential. Your use of mHealth can improve the quality of the health information being captured, educate you about relevant health issues, monitor your fitness progress, or help you remember when to take certain medications.

What Are The Privacy Risks Associated With Using mHealth Technology?

215 million mobile device sales are expected to be made in 2016, and mobile device users who downloaded at least one health app to their smartphones doubled between 2011 and 2012.[2] The numerous mHealth options available to consumers can be overwhelming, leading many to simply select the most popular app or purchase multiple wearables in an effort to determine which one might work best for them. Moreover, the information collected through your smartphone, tablet, or wearable can be quite personal and sensitive, such as name, height and weight, pregnancy status, chronic medical condition, real-time location, and even menstrual cycles. The novelty, variety, and complexity of this particular technology creates unique privacy risks for patients.

In 2015, consumer mHealth apps targeting wellness (fitness, lifestyle & stress, diet & nutrition) comprised 2/3 of mHealth app space.

What many consumers may not know is that a large majority of app and mHealth software developers are not subject to laws governing the privacy of personal health/medical information the way health care providers are. Each time you use a mHealth "tool" (e.g., a weight loss or mental health app or activity tracker), you create a record of information that likely "has no regulatory protection."[3] The only privacy protections you may have may appear in the app or software developer's privacy policy, if such a policy exists at all. Before downloading a health app or texting your doctor, you should be aware of the privacy and security risks associated with using mHealth technology. This patient/consumer guide will focus on the privacy and security aspects of using mHealth technology and provide practical advice on how to protect against such risks.

Tips for Protecting Your Privacy in an mHealth World

Even if a privacy policy exists for the mHealth app, wearable, or software you want to use, the app may have “poor security,” which means your health information may be shared or transmitted unencrypted over an unsecured network connection (an unsecure network connection is indicated by “http://” rather than “https://”).[4] Encryption is the process of converting information or data into a cipher or code so that only authorized parties can read it.

The information being shared may even include the search terms you use to learn more about a certain drug, immunological disorder, or sexually transmitted disease that, if searched on an unsecure network, can be “viewable by anyone watching on the network.”[5] In addition, using public Wi-Fi networks (e.g., your public library or local coffee shop) to send or receive health information can be an easy way for unauthorized users to intercept information. Finally, lost or stolen devices represent a major risk for breach of privacy.

1 in 10 mHealth apps has the capacity to link to a “wearable” such as Fitbit®, “smart socks,” and devices that attach to asthma inhalers.

Given the number of mHealth technology options that are instantly available to you through your smartphone, tablet, or wearable—and the opportunities through which the privacy and security of your health information can be compromised—the following sections provide practical tips for you to consider and questions to ask before you enable your activity tracker, download a blood pressure app, or email a photo of a skin rash to your doctor.

Your Mobile Device

◊ *Authentication*—Does your mobile device enable “authentication,” which is the process of verifying your identity and/or your device to ensure secure access?

◊ *Encryption*—Does your mobile device have built-in encryption capabilities? If not, you can purchase and install encryption software for your device.

◊ *Remote Wiping & Disabling*—Does your mobile device have remote wiping and/or disabling capabilities? If your device gets stolen or lost, remote wiping/disabling allows you to lock and/or erase your data remotely.

◊ *Password Protection*—Requiring a password to access your mobile device provides an initial layer of security should your device get lost or stolen.

◊ *Software Updates*—A determined hacker may still be able to pierce through all of the security measures you have undertaken for your mobile device (e.g., password protection, authentication, installment of encryption software, remote wiping and disabling capabilities). It is therefore important that you update all appropriate antivirus software and firewalls on a regular basis.

◊ *The Device’s Warranty*—Review your mobile device’s warranty and support policies to see if security and software patches are provided for the life of your product.

◊ *Wi-Fi Hot Spots*—Consider using health apps on your mobile device only if you can ensure an encrypted and secure connection. As mentioned earlier, unauthorized users can view or intercept your information in public wi-fi hot spots.

- ◊ *Important Note About Mobile Devices*—mHealth devices are not limited to smartphones, tablets, and wearables. Certain mobile medical devices that are connected to the Internet, such as infusion pumps and implantable biosensors (e.g., cardiovascular defibrillators), are also at risk of being hacked by unauthorized users, potentially compromising patient care. Given the complexity of such devices and the software needed to operate them, you should immediately install any software updates that arise.

Your Mobile Health App

- ◊ *Your Comfort Level*—Are you comfortable with the level of personal information that a particular health or wellness/fitness app is requesting? It is very likely that free apps, which depend on advertising revenue, will distribute your information to the app developer, third-party sites that the app developer uses, and to unidentified third-party marketers and advertisers.[6]

◊ *Do Your Homework*—Before downloading an app, research the app as much as you can:

- Read other users' reviews about the app.
- See if the app was mentioned in any media/news stories.
- Read the privacy policy associated with the app. If none seems to exist, see if the app developer has a privacy policy on its website. Also, look to see if the app has a policy on its data collection practices, as well as a policy on the sharing of your information with third parties.
- Find out what "permissions" the app is requesting and disable the ones that are not necessary for the app to function. For example, if your app does not need location-enabling services to function properly, you can disable or turn off that particular permission.
- If possible, "test-drive" the app first before entering your personal information.
- For maximum privacy, consider using only paid apps. An app that does not rely on advertising revenue is less likely to share your information with marketers and other third parties.

Your Data

◊ *Data Storage*—Determine where your data is being stored: In your mobile device? Personal home computer? Work computer? In the computer system of your doctor's office? A third party's computer system, such as "the cloud"? The privacy policies for each location in which your data is stored may differ.

The typical text messaging app does not offer the security needed when protected health information is being transmitted.

◊ *Meaningful Use Requirement*—The "Meaningful Use Requirement" is a federal government incentive program for health care providers that requires providers to use certified electronic health record (EHR) technology to achieve certain patient-centered goals, including protecting the privacy and security of the patient's health/medical records. If your physician's practice meets the Meaningful Use security requirements for EHR, your doctor is likely to have security measures in place that will protect the privacy and security of your personal health information.

◊ *Delete Your Apps*—If you are no longer using the app, delete it from your mobile device and, if possible, delete your personal profile and the data archive you've created.

Communicating With Your Doctor

A large part of using mHealth technology can involve communicating with your physician by email or text, but if those emails and texts are transmitted through an unsecured network, you risk compromising your privacy.

Email

Health care providers are allowed to communicate with you through unencrypted email as long as reasonable safeguards are applied, such as double-checking the patient's email address, sending an email alert first so that the patient can confirm that his/her email address is correct, and limiting the amount or type of medical information being disclosed in the email. However, if you do not feel comfortable with this, your health care provider must provide you with alternative means of communication, such as telephone, regular U.S. mail, or using a more secure electronic method of communication, such as the patient portal.[7]

If the patient initiates the email to his/her doctor, the doctor may assume that email is an acceptable form of communication for the patient, but if the health care provider believes the patient is unaware of the risks associated with using email and/or is concerned about potential liability, the provider can alert and inform the patient of those risks and let the patient decide whether to continue communicating by email.[8]

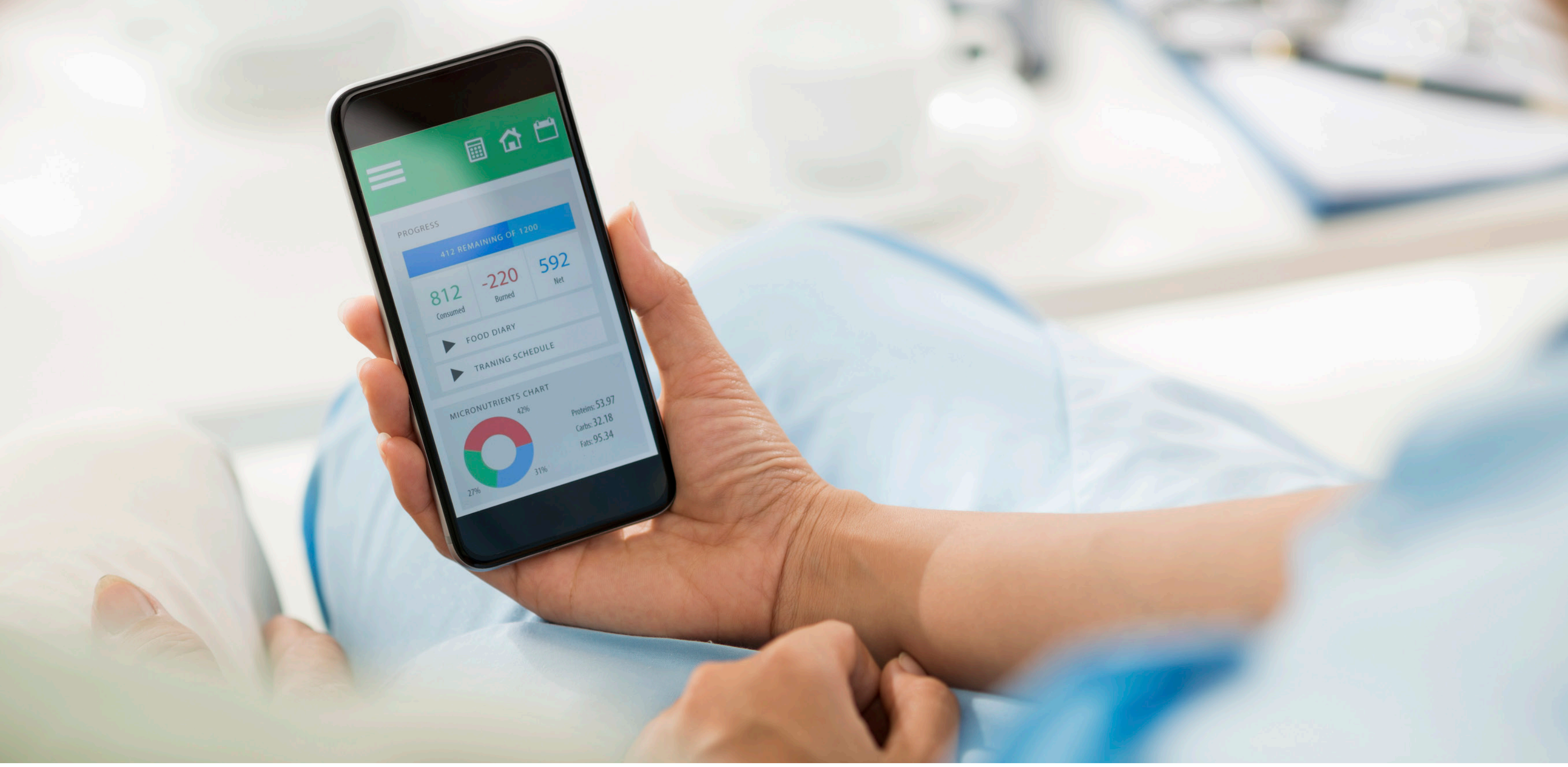
Practical Tips on Emailing Your Doctor

- ◊ When emailing with your doctor, use your personal email address rather than your office/work email address. In most cases, your employer owns the content found on your work computer, which can be accessed by your employer at any time.

- ◊ If the content of your email includes information that is relevant to your health care (e.g., diagnosis, monitoring of symptoms, course of treatment, medication changes, etc.), your doctor will likely make the email a part of your medical record.

- ◊ If your doctor chooses not to communicate your medical or health information over email, it may be due to security concerns, the sensitive nature of the information, or your doctor preferring to share important test results in person so that you can ask questions right away.

- ◊ Emailing your doctor is never suitable during a medical emergency.



The Patient Portal

An increasing number of physician groups and hospitals are inviting their patients to create an online account through a "patient portal," which is basically a website that you can access from virtually anywhere using your smartphone, tablet, or other mobile communication device. A patient portal allows you to:

- Securely exchange information and communicate with your health care provider.
- Request medication refills.
- Schedule a future appointment or check-in for an upcoming appointment.
- Be reminded about an upcoming appointment.
- View educational materials about a certain medical condition.
- Receive your test results.
- Review or obtain information directly from your electronic health record.

Access to your patient portal requires your user ID and password. Patient portals do not store the information on your own home/personal computer or mobile device, thereby providing a stronger layer of security than if you were to communicate with your physician by regular email or text.

Texting Between Health Care Providers and Patients

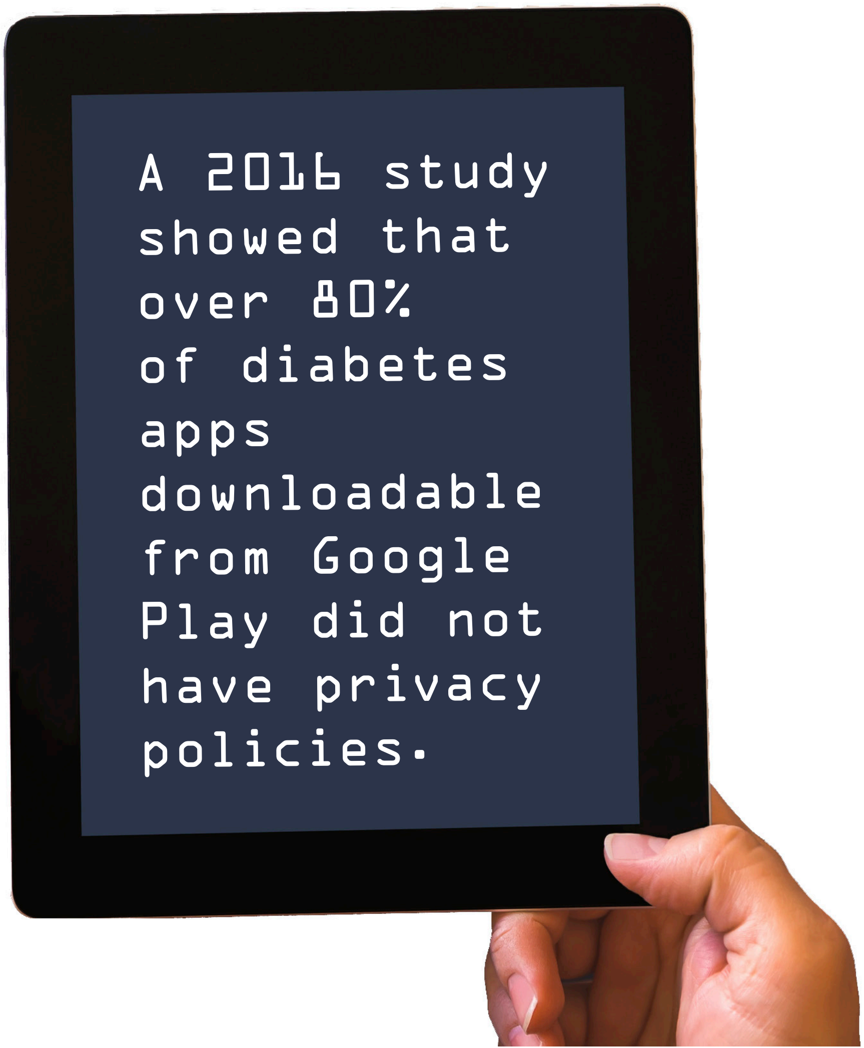
The simplicity and efficiency of texting makes this an appealing way for doctors to communicate with patients and vice versa. However, text messaging has significant privacy and security risks.

For example, if your device is stolen, lost, or discarded, anyone can easily access the messages without having to use a password or some other form of authentication. When you send a text, you cannot be certain that the text is being read by the intended recipient. Security is further limited because text messages from most devices are not encrypted.

For the reasons above, texting in clinical settings has been limited as arguably even appointment reminders sent via text could violate a patient's privacy. However, the development of secure mobile messaging platforms for medical practices has made it possible for providers to send texts to one another and to patients without violating privacy laws.

Medical practices that have adopted these platforms will generally offer you the option of receiving appointment reminders or sending basic questions to your doctor via text and require you to sign an agreement that you accept to communicate via text. The agreement should explain the practice's policies with respect to the type of information texts may contain, password and encryption standards for the devices that are used for texting, the addition of texts to the patient's medical record, and how and when the texts are deleted.

As a patient, you may also be asked what type of information you are willing to transmit or receive via text and who has access to your phone. You may also be asked to agree to delete the messages once you have read them and to notify the practice in writing if you change your phone number or acquire another device.



A 2016 study showed that over 80% of diabetes apps downloadable from Google Play did not have privacy policies.

If you are not comfortable using texting as a method of communicating with your health care providers, alternate methods of communication are always available and can be specifically requested.

For more information about communicating with your health care provider, check your state's department of health or medical board website for information about patient privacy, rights to your health information, and communicating with your health care providers. A list of internet patient resources offered by the federal government includes information about your rights under the Health Insurance Portability and Accountability Act (HIPAA) and HIPAA for individuals.

Conclusion

Mobile health technology is here to stay, and the potential benefits of using it are enormous. At the same time, the privacy and confidentiality of the health information we knowingly or unknowingly provide through our mobile communication devices can be compromised if we're not careful about knowing as much as we can about the devices we use and the mHealth tools we download or purchase. Taking what steps you can to protect your privacy while your health information is being collected, recorded, stored, shared, and/or analyzed will help you make the most of your mHealth options.

ENDNOTES

[1] New report finds more than 165,000 mobile health apps now available, takes close look at characteristics & use, iMedical Apps, www.imedicalapps.com.

[2] mHealth in an mHealth World: How mobile technology is transforming health care, Deloitte, at http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-mhealth-in-an-mworld-103014.pdf

[3] Mobile Health and Fitness Apps: What Are the Privacy Risks? Privacy Rights Clearinghouse, www.privacyrights.org.

[4] Id.

[5] Id.

[6] Mobile Health and Fitness Apps: What Are the Privacy Risks? Privacy Rights Clearinghouse, at https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks#section

[7] Does the HIPAA Privacy Rule allow permit health care providers to use e-mail to discuss health issues and treatment with their patients? http://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/

[8] Id.

FACTOID SOURCES

Page 4: Patient Adoption of mHealth: Use, Evidence and Remaining Barriers to Mainstream Acceptance, IMS Institute for Healthcare Informatics (Sept. 2015), Pg. 4 at http://www.imshealth.com/en/thought-leadership/ims-institute/reports/patient-adoption-of-mhealth.

Page 5: Patient Adoption of mHealth: Use, Evidence and Remaining Barriers to Mainstream Acceptance, IMS Institute for Healthcare Informatics (Sept. 2015), Pg. 14 at http://www.imshealth.com/en/thought-leadership/ims-institute/reports/patient-adoption-of-mhealth.

Page 8: Jon Jansen, mHealth Will Drive Physician Demand for Secure Text Messaging in 2014 (Jan. 8, 2014), at http://hitconsultant.net/2014/01/08/mhealth-will-drive-physician-demand-for-secure-text-messaging-in-2014/.

Page 12: Mobile health Apps Continue to Make Headlines (March 2016), at https://www.healthlawpolicymatters.com/2016/03/16/mobile-health-apps-continues-to-face-privacy-security-and-consumer-protection-issues/.

Authors

The American Health Lawyers Association is grateful to the following authors, project leaders, and peer reviewers for their expertise and contributions to this publication.

Nancy P. Gillette
General Counsel
Ohio State Medical Association
Dublin OH
gillette@osma.org

Rick L. Hindmand
Member
MacDonald Hopkins LLC
Chicago IL
rhindmand@mcdonaldhopkins.com

Sarah T. Hogan
Partner
McDermott Will & Emery LLP
Boston MA
shogan@mwe.com

Patricia A. Markus
Partner
Nelson Mullins Riley & Scarborough LLP
Raleigh NC
trish.markus@nelsonmullins.com

David G. Parks
Compliance and Privacy Officer
Lutheran Medical Center & Good Samaritan
Medical Center
SCL Health
Broomfield CO
david.parks@sclhs.net

Fredric E. Roth V
Associate
Thompson Coburn LLP
Chicago IL
froth@thompsoncoburn.com

Andrew A. Schillinger
Dir. of Risk Management & Compliance
Inland Northwest Health Services
Spokane WA
schilla@inhs.org

Elizabeth Skinner
Regional Corporate Responsibility Officer
Florida Hospital Medical Group
Maitland FL
elizabeth.skinner@flhosp.org

Alison C. Sorkin
Associate General Counsel
University of Colorado Health
Aurora CO
alison.sorkin@uchealth.org

Marcie R. Swenson
Regional Compliance Administrator & Attorney
Intermountain Healthcare
Salt Lake City UT
marcie.swenson@imail.com

David S. Szabo
Partner & Co-Chair, Healthcare Practice Group
Locke Lord LLP
Boston MA
David.szabo@lockelord.com

Ashley L. Thomas
Associate
Nelson Mullins Riley & Scarborough LLP
Raleigh NC
ashley.thomas@nelsonmullins.com

Special Thanks to Our Public Interest Donors

This publication was made possible by the generosity of AHLA's Public Interest Donors. Donors who contributed $100 or more between January 1, 2016 and July 31, 2016 are recognized here for their support. For a complete list of all AHLA Public Interest Donors, please visit www.healthlawyers.org/donors.

Visionary
($2,500 or more)
Anonymous
Theodore N. Giovanis

Leader
($1,500–$2,499)
Jay A. Martus
Kathy L. Poppitt
Glen A. Reed
Sanford V. Teplitzky
Mary Jane Whitt
Teresa A. Williams

Benefactor
($1,000–$1,499)
Douglas A. Hastings
Kerry Beth Hoggard
S. Craig Holden
David E. Matyas
Kristen B. Rosati
Eric Zimmerman

Patron
($500–$999)
James W. Boswell
Jennifer R. Breuer
Curt J. Chase
Almeta E. Cooper
Lois Dehls Cornell
Dawn R. Crumel
Paul R. DeMuro
Robert G. Homchick
James P. Kelly
Christine A. Lay
Arthur N. Lerner
Kim Harvey Looney
Douglas M. Mancino
David Marx, Jr
Hal McCard
Barbara L. Miltenberger
Robert R. Niccolini
Maria Nutile
Dorthula H. Powell-Woodson
Cynthia Y. Reisz
Robert L. Roth
Edward F. Shay
Thomas N. Shorter
Toby G. Singer
Patrick D. Souter
Harvey M. Tettlebaum

Contributor
($250–$499)
Timothy B. Adelman
Gail B. Agrawal
Gregory D. Anderson
Jerry A. Bell, Jr
Ann M. Bittinger
Mark A. Bonanno
H. Guy Collier
Thomas W. Coons
Dale H. Cowan
Richard G. Cowart
Claire Cowart Haltom
Thomas S. Crane
Anthea R. Daniels
Todd M. Ebersole
James F. Flynn
Elaine M. Gerson
Marc D. Goldstone
Joel M. Hamme
Douglas J. Hammer
Anne W. Hance
Lisa A. Hathaway
Michael C. Hemsley
Leonard C. Homer
Alan C. Horowitz
Thomas K. Hyatt
John R. Jacob
Laura F. Laemmle-Weidenfeld
Robert F. Leibenluft
Amy S. Leopard
Gregory M. Luce
Patricia A. Markus
Thomas Mayo
Eric J. Neiman
Peter A. Pavarini
Michael D. Phillips
Rebekah N. Plowman
Kathleen M. Premo
Nancy Jill Reed
Richard L. Shackelford
Brenda Eady Stafford
T.J. Sullivan
Richard F. Tompkins
Robert E. Weatherford
Matthew E. Wetzel
Lois Wischkaemper
Heather M. Zimmerman

Friend
($100-$249)
S. Allan Adelman
Michael F. Anthony
Xavier Baker
Dennis M. Barry
Curtis H. Bernstein
Michael J. Bittman
Stephen M. Blaes
Christi J. Braun
George B. Breen
Jason E. Bring
Teresa Meinders Burkett
Richard Ross Burris, III
Kathy H. Butler
Michael R. Callahan
Terri Wagner Cammarano
Elizabeth Rada Carver
Charlotte A. Combre
Jane Reister Conard
Michael H. Cook
Ritu Kaur Cooper
Evan A. Coppola
Anne E. Cramer
Maria Greco Danaher
James M. Daniel, Jr
Benjamin Martin Daniels
Gary Scott Davis
Nicole F. DiMaria
Petra Lee Dodd
Barbara J. Duffy
Heidi Y. Echols
Amanda L. Enyeart
Kimberly Everett
Andrea M. Ferrari
Michael N. Fine
Donna D. Fraiche
Robert Andrew Gerberry
Lisa J. Gilden
Nancy P. Gillette
Eric B. Gordon
Alice G. Gosfield
Michael R. Greer
Emily Black Grey
Anna M. Grizzle

Leah B. Guidry
Susan K. Hackney
Kristen A. Harris
Gail D. Hasbrouck
Scot T. Hasselman
Robyn L. Helmlinger
Rick L. Hindmand
John R. Holdenried
Ann T. Hollenbeck
William W. Horton
Jennifer C. Hutchens
Jennifer Wooten Ierardi
Travis F. Jackson
Andrea M. Kahn-Kothmann
Jeffrey L. Kapp
Julie E. Kass
Peter M. Kazon
John E. Kelly
Susan Kendig
Geralyn A. Kidera
Cavender C. Kimble
Richard G. Korman
Marilyn Lamar
Kimber L. Latsha
Aletheia Lawry
Joanne R. Lax
Lewis A. Lefko
David T. Lewis
McKenzie A. Livingston
William T. Mathias
Peter M. Mellette
Joel L. Michaels
Gregory J. Minana
Jeffrey S. Moore
Linda Sauser Moroney
Robin Locke Nagele
Dinetia M. Newman
James Franklin Owens
Robert A. Pelaia
Christopher C. Puri
Deborah A. Randall
Mary Holloway Richard
Matthew B. Roberts
Vicki L. Robinson
James Roosevelt, Jr
Rachel Veronica Rose

Linda S. Ross
Fay A. Rozovsky
Kimberly S. Ruark
James A. Saling
Ross E. Sallade
Alan E. Schabes
Beth J. Schermer
Susan O. Scheutzow
Kendall A. Schnurpel
Jeffrey B. Schwartz
Asha B. Scielzo
Jeff Sconyers
Suzanne J. Scrutton
Albert W. Shay
Jeffrey W. Short
Gerald M. Sill
Julie A. Simer
H. Terrence Smith
Rachel Spitz
Ross E. Stromberg
Sarah E. Terrace
Robert J. Tomaso
James L. Touse
Cori Casey Turner
Lisa Diehl Vandecaveye
Lawrence W. Vernaglia
Glenn J. Waldman
Howard T. Wall, III
Judith A. Waltz
David A. Weil, II
Kristian Andrew Werling
Charles R. Whipple
Christine L. White
Kathryn K. Wire
Ivan Wood, Jr
Kristen McDermott Woodrum
Janice H. Ziegler

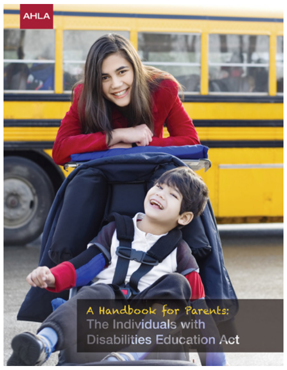
AHLA 50 1967-2017

Additional Public Interest Resources

Medicaid Basics: Eligibility, Coverage, and Benefits

Provides answers to the most commonly-asked questions about Medicaid's background, history, coverage, and eligibility requirements.

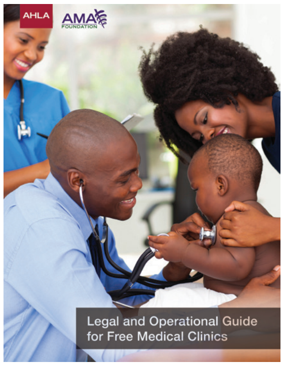
www.healthlawyers.org/MedicaidBasics



A Handbook for Parents: The Individuals with Disabilities Education Act

Addresses the educational challenges that parents and caretakers of children with disabilities face and offers valuable guidance about rights and benefits.

www.healthlawyers.org/IDEA



Legal and Operational Guide for Free Medical Clinics

Gives clinic organizers a broad understanding of the numerous and most commonly encountered legal and operational issues that must be taken into consideration when starting a free or charitable medical clinic.

www.healthlawyers.org/FreeMedicalClinic

FREE DOWNLOAD!

ONLINE AT

www.healthlawyers.org/publicinterest