PATIENT PRIVACY IN A MOBILE WORLD

A FRAMEWORK TO ADDRESS PRIVACY LAW ISSUES IN MOBILE HEALTH

JUNE 2013

TrustLaw CONNECT
A THOMSON REUTERS FOUNDATION SERVICE

mHealth Alliance

BAKER & MCKENZIE

MSD Be well

PATIENT PRIVACY IN A MOBILE WORLD

A FRAMEWORK TO ADDRESS PRIVACY LAW ISSUES IN MOBILE HEALTH

JUNE 2013

TrustLaw CONNECT
A THOMSON REUTERS FOUNDATION SERVICE

mHealth Alliance

BAKER & McKENZIE

MSD
Be well

ACKNOWLEDGEMENTS

Thomson Reuters Foundation and the TrustLaw Connect team are truly grateful to each of the partners that contributed to and collaborated on this work:

mHealth Alliance identified the need to examine this important issue and brought their expertise on mobile health in the global arena. We truly value their collaborative approach and ability to engage with multiple stakeholders to deliver this project.

Baker & McKenzie and **Merck** dedicated significant resources as the international coordinators for this project, bringing a wealth of legal and commercial expertise on health, privacy and data protection laws. Baker & McKenzie also carried out the research for the Chilean and Peruvian case studies in this report.

Doulah & Doulah for the Bangladesh research, MMAKS for the Ugandan research, Nisith Desai for the Indian research, Templars for the Nigerian research and Ubena John, Doctoral Candidate at Stockholm University for the Tanzanian research.

The mHealth Alliance wishes to acknowledge a number of individuals who contributed to the production of this publication. First, we would like to thank Kathy Calvin, President and CEO of the United Nations Foundation, whose initial conversations with Monique Villa, President of the Thomson Reuters Foundation, led to the development of the TrustLaw Connect project that forms the basis for this publication. We also want to acknowledge and thank Patricia Mechael, Executive Director of the mHealth Alliance, whose leadership in addressing concerns around privacy, confidentiality and data security as key

barriers to using mobile technology launched the work of the Alliance and led to the engagement with Thomson Reuters Foundation, Baker & McKenzie and Merck. The Alliance also wishes to thank William Philbrick, who, on behalf of the Alliance, oversaw and managed the project that led to this publication. His efforts were part of a larger team effort that included Chelsea Hedquist, Jon Payne, Madhu Deshmukh, Shariq Khoja, Avrille Hanzel, Adele Waugaman, Madhura Bhat, Francis Gonzales, Chelsea Solmo and Sarah Struble.

BAKER & McKENZIE

Baker & McKenzie is proud to contribute to this paper and the efforts of the mHealth Alliance in championing the use of mobile technologies to improve health throughout the world. A very special thank you is due to the TrustLaw Connect network of the Thomson Reuters Foundation for organizing the project and undertaking the process of assembling the contributing lawyers. Baker & McKenzie is deeply grateful to Merck and its global team for co-leading this project and providing constant input and support. Also, this paper could not have been completed without the essential contributions of Doulah & Doulah from Bangladesh, MMAKS Advocates from Uganda, Nisith Desai Associates from India, Templars from Nigeria and Ubena John from Tanzania. Finally, we would like to thank the following individuals who comprised our global team: Michael J. Wagner (Chicago), Brian Hengesbaugh (Chicago), Karen Sewell (Chicago), Kate O Suilleabhain (Chicago), Amy de La Lama (Chicago), Peter R. George (Chicago), Lindsay M. Martin (Chicago), Jacqueline M. Wilkosz (Chicago), Deanna Bougie (Chicago), Erin Boo (Chicago), Teresa Tovar (Lima), Jorge Ossio (Lima), Viviana Chavez (Lima), Christoph Rittweger (Munich), Julia Wendler (Munich), Katherine T. Sakoda (Palo Alto), Antonio Ortuzar, Jr. (Santiago), and Rafael Pastor (Santiago).

MSD *Be well*

Merck wishes to express appreciation to both the mHealth Alliance and the TrustLaw Connect network of the Thomson Reuters Foundation for the opportunity to work on this important project, as well as the

excellent collaboration by both organizations throughout its planning and implementation. In addition, we wish to acknowledge the invaluable contribution made by Baker & McKenzie as well as the other participating law firms. Finally, but not least, we at Merck are very proud of the contribution made to the project by a global team including colleagues from our Office of General Counsel and Global Compliance Organization, in several locations in the US, Europe and Asia Pacific regions. As such, this project is an important milestone in the ongoing expansion and globalization of Merck's long standing legal pro bono program.

Since 1965 Doulah & Doulah
ADVOCATES, ATTORNEYS & NOTARIES

We acknowledge the contribution of all of the partners involved in the project and especially Nasir and Amina, partners at Doulah & Doulah, for the local research. Special thanks go to Karen Sewell at Baker & McKenzie and Serena Grant and Dianne Marcos at the Thomson Reuters Foundation for taking up the toughest job of cross-border co-ordination and consolidation.

MASEMBE, MAKUBUYA, ADRIKO,
KARUGABA & SSEKATAWA ADVOCATES
(MMAKS ADVOCATES)

ALN

MMAKS Advocates acknowledges the work of Mr. Phillip Karugaba and Ms. Gloria Matovu who volunteered on the mHealth Alliance Research.

TEMPLARS

We would like acknowledge the following members of the Templars team — Olumide Akpata, Ijeoma Uju, Chioma Oparadike, Oyeyemi Immanuel and Ebuka Uyanwa — for their contributions to this project.

DISCLAIMER

The material in this paper is of the nature of general comment only and is not intended to be a comprehensive exposition of all potential issues, nor of the law relating to such issues. It is not offered as advice on any particular matter and should not be taken as such. The precedent documents included in this paper have not been prepared with any particular matter in mind. Baker & McKenzie, Merck, Thomson Reuters Foundation, the editors and the contributing authors disclaim all liability to any person in respect of anything done and the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or part of this paper. Before any action is taken or decision not to act is made, specific legal advice should be taken in light of the relevant circumstances and no reliance should be placed on the statements made or documents reproduced in this paper.

TABLE OF CONTENTS

SELECTED DEFINITIONS

mHEALTH: Although there is no uniform definition of "mHealth," the term generally connotes mobile health as medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices; mHealth involves the use and capitalization on a mobile phone's core utility of voice and short messaging service (SMS) as well as more complex functionalities and applications including general packet radio service (PRS), third and fourth generation mobile telecommunications (3G and 4G systems), global positioning system (GPS), and Bluetooth technology

eHEALTH: eHealth covers all uses of network-based information and communication technology to promote longer, healthier lives

INFORMATIONAL PRIVACY: an individual's right to control the acquisition, use, and disclosure of identifiable health data

CONFIDENTIALITY: refers to the obligations of those persons who receive mHealth data to preserve secrecy of information entrusted to them and use it only as instructed by the patient and/or as necessary to provide the services for which the patient entrusted the information to this person.

INFORMATION SECURITY: physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure, including security of wireless networks, security of devices, applications security, back-end systems security, and secure user practices.

GSM vs. CDMA: CDMA (Code Division Multiple Access) and GSM (Global System for Mobiles) are shorthand for the two major radio systems used in mobile phones. The United States is a largely a CDMA-based mobile phone market, while Europe and the rest of the world have largely embraced GSM. Generally, phones built for one system do not work on the other system and vice versa. The technology behind each system offers certain default capabilities (such as simultaneous voice and data for GSM) and other distinctions that can impact interoperability and standardization across mobile networks.

API: An application programming interface is a protocol intended to be used as an interface by software components to communicate with each other.

ACRONYMS

AMA	American Medical Association
API	Application programming interface
APP	Australian Privacy Principles
BMA	Bangladesh Medical Association
CDC	Centers for Disease Control and Prevention
CDMA	Code Division Multiple Access
CEMAC	Code of Ethics of the Medical Association of Chile
COPPA	Children's Online Privacy Protection Act of 1998 (US)
FTC	Federal Trade Commission (US)
FTC ACT	Federal Trade Commission Act (US)
GHL	General Health Law (Peru)
GMC	General Medical Council
GPS	Global Positioning system
GSM	Global System for Mobiles
HHS	Health and Human Services (US)
HIPAA	Health Insurance Portability and Accountability Act of 1996 (US)
IFAI	Institute for Access to Information and Personal Data
ITA	Information Technology Act, 2000 (India)
LFPDP	Ley Federal de Proteccion De Datos Personales en Posesion de los Particulares (Mexico)
MCI CODE	Indian Medical Council
OECD	Organisation for Economic Co-operation and Development
PDAs	Personal digital assistants
PDPA	Personal Data Protection Act (Singapore)
PDPL	Personal Data Protection Law (Argentina)
PHI	Protected health information

PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PRS	Packet radio service
PSQIA	Patient Safety and Quality Improvement Act (US)
ROHSL	Law No. 20.584, The rights and obligations of people in regards to actions connected to their health service) (Chile)
SCA	Stored Communications Act (US)
SMS	Short messaging service
UIDID	Unique Device Identifiers
UNF	United Nations Foundation
WHO	World Health Organization

FOREWORD

Thomson Reuters Foundation is proud to present this TrustLaw report on "**Patient Privacy in a Mobile World – A Framework to Address Privacy Law Issues in Mobile Health**". This work is the result of collaboration with the mHealth Alliance, hosted by the United Nations Foundation, international law firm Baker & McKenzie and global healthcare provider Merck together with local counsel in each of the case study countries.

The Thomson Reuters Foundation leverages the skills, values and expertise of Thomson Reuters to run programmes that trigger change and empower people across the world: free legal assistance, media development, and in-depth coverage of the world's under-reported stories. The Foundation stands for human rights, women's empowerment, anti-corruption and for the rule of law. TrustLaw Connect is the Thomson Reuters Foundation's global pro bono service that amplifies the impact of NGOs and social enterprises by connecting them with the best lawyers around the world. Its mission is to spread the practice of pro bono worldwide to drive social change.

When the mHealth Alliance first proposed the concept for this project to examine the protection of patient privacy in the context of mobile health, we immediately recognised it as a wonderful opportunity to bring together some of the best legal minds from around the globe to address this pressing issue. A recent United Nations study showed that more people now have access to a mobile phone than to a toilet, which obviously has huge implications for the growth of mHealth.

It is paramount that privacy concerns are addressed as the field grows, to ensure that health information is not used to patients' detriment, particularly those who are vulnerable to discrimination.

We hope that this report will be a useful tool for legislators, policymakers, telecommunications companies and healthcare providers to identify the policy gaps and the legal and technological changes that need to be addressed in order to strengthen privacy laws that relate to mobile healthcare.

MONIQUE VILLA
CEO, Thomson Reuters Foundation

EXECUTIVE SUMMARY

Amid the rapid growth of mobile network technology and infrastructure throughout the world, especially in low- and middle-income countries, the potential of mobile to support the achievement of health priorities is an area of active exploration and engagement. According to a 2011 World Health Organization report, governments cite issues related to data privacy and security and the protection of individual health information as two of the top barriers to the expansion of mHealth. Protecting personal health information that is collected and transmitted over mobile devices is essential to bringing mHealth to scale and providing a mature foundation for its continued growth.

The mHealth Alliance, the Thomson Reuters Foundation, Merck, and Baker & McKenzie partnered on a project to better understand privacy and security policy issues related to mHealth and identify gaps that must be addressed to protect health data. The partnership undertook a global landscape analysis of current privacy legislation and regulation was undertaken, with a closer look at a selected group of case study countries in Africa, Asia and Latin America, to establish a baseline for the discussion and provide examples of what different approaches to privacy regulation are already in use. The results of this review show that the world of privacy law is roughly divided into three major camps: (1) omnibus data protection regulation in the style of the European laws that regulate all personal information equally; (2) U.S.-style sectoral privacy laws that address specific privacy issues arising in certain industries and business sectors, so that only certain types of personal information are regulated; and (3) the constitutional approach, whereby certain types of personal information are considered private and inviolate from a basic human rights perspective but no specific privacy regulation is in place otherwise.

Among the new laws that have been adopted in recent years, the European omnibus approach has been the most popular. This may be attributed at least in part to the cross-border transfer restrictions found in the European laws, which allow free transfer of personal information across borders only to those countries deemed to have "adequate" data protection regulation in place (i.e. laws similar to those found in Europe). To date, the European Commission has recognized the adequacy of privacy laws in Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Jersey, the Isle of Man, Switzerland, Uruguay and the U.S. Department of Commerce Safe Harbor Privacy Principles. However, for the rest of the world, this style of law poses an additional barrier to the cross-border transfer of personal information, an issue that is especially relevant to mHealth and its many transnational aspects.

Otherwise, this paper summarizes the other major aspects of current laws to provide a snapshot of where the laws stand today and a baseline for discussing potential reform and the adoption of new laws. Interestingly, very few of the existing laws cover health information specifically (the United States being the prime exception) and fewer still make any reference, even in terms of regulatory guidance, to mHealth. The current application of these privacy laws to mHealth issues, therefore, is by extension of existing, more general principles related to privacy protection. For this reason and to provide more specific examples that can be used to address mHealth privacy issues, this paper also offers an overview of medical ethics and patient confidentiality codes in effect throughout the world.

This paper then goes on to set forth a functional framework for addressing privacy law issues around the globe, which adapts and is sensitive to particular cultural, technological and institutional contexts. The main pillars of the framework are: (1) **fact gathering** and **analysis** that aim to identify the key drivers for privacy regulation in a particular jurisdiction and the existing environment for the development of such laws; (2) determining **scope of coverage** in a thoughtful and deliberate manner that takes into account the results of the fact-gathering stage and the potential impact of scoping decisions on the further uptake of mHealth in a particular jurisdiction; (3) deciding the nature of any **notice and consent** requirements built into the privacy law reflecting the cultural and technological context of the jurisdiction where the law would be implemented; (4) incorporating the principle of **data minimization** into any law as a best practice; (5) encouraging the right of **data integrity and accessibility** for data subjects while requiring such requests to be commercially reasonable and feasible for the entities storing data to honor; (6) requiring the adoption of reasonable **data security** measures while remaining nimble and open to new technological advances in this area; (7) ensuring that data is protected throughout its lifecycle through **cross-border and third-party transfer restrictions**, while being sensitive to the operational burdens such restrictions could place on market participants and the consequences for the uptake of mHealth; (8) determining the **enforcement and sanctions** mechanisms built into the law to credibly encourage compliance, which also requires an honest assessment of the jurisdiction's enforcement resources.

The hope is that the work undertaken here can provide a working taxonomy and toolbox for those who continue to explore and develop these issues in the coming months and years. It is worth noting that this paper does not set out to prescribe legal solutions to specific data privacy problems or advocate for one universal model law for the entire world. The authors believe that a one-size-fits-all approach is simply not appropriate in the privacy context and much less in an environment, such as mHealth, where the technology and the issues are still evolving every day.

INTRODUCTION

Today the ubiquity of mobile phone technology is undeniable. The World Bank reported that the number of mobile subscriptions in use worldwide, both pre-paid and post-paid, has grown from fewer than 1 billion in 2000 to over 6 billion in 2012 (current world population estimates are near 7 billion).[1] Other reports show that mobile penetration rates in Africa, Asia-Pacific and Latin America are expected to reach 82%, 98% and 120% respectively in 2014.[2] In fact, some developing countries such as Algeria, Botswana, Brazil, Chile, Indonesia and Malaysia have already crossed the 100% mobile penetration mark.[3] Cisco reports worldwide 48 million people without electricity and landline Internet access have a mobile phone, showing that mobile use outpaces basic infrastructure in many rural and developing areas.[4] Mobile telephony's reach in the developing world is presenting innovative and promising solutions, such as with the mobile-based money transfer system in Kenya, M-Pesa, and, more broadly, mobile health technology, the subject of this paper.

The use of mobile and wireless technologies to support the achievement of health objectives ("mHealth") has been

1 The World Bank, Mobile Phone Access Reaches Three Quarters of Planet's Population (July 17, 2012), at **http://www.worldbank.org/en/news/press-release/2012/07/17/mobile-phone-access-reaches-three-quarters-planets-population**.

2 GSM Association, *Touching Lives Through Mobile Health: An Assessment of the Global Market Opportunity*, available at **http://www.pwc.in/assets/pdfs/telecom/gsma-pwc_mhealth_report.pdf** (Feb. 2012).

3 GSM Association, *Touching Lives Through Mobile Health: An Assessment of the Global Market Opportunity*, available at **http://www.pwc.in/assets/pdfs/telecom/gsma-pwc_mhealth_report.pdf** (Feb. 2012).

4 Janet Maragiolio, Mobiledia, The Future of Medicine: Wiping Out Third World Diseases (Feb. 10, 2012), at **http://www.mobiledia.com/news/127632.html**.

identified by global institutions as having "the potential to transform the face of health service delivery across the globe."[5] Of the 114 member states completing a 2009 survey conducted by the World Health Organization's ("WHO") Global Observatory for eHealth, 83 percent reported offering at least one type of mHealth service, with many countries offering four to six programs. Amongst the most frequently reported mHealth initiatives were: health call centers (59%), emergency toll-free telephone services (55%), managing emergencies and disasters (54%), and mobile telemedicine (49%).[6] At the United Nations Summit on the Millennium Development Goals in September 2010, Secretary-General Ban Ki-moon launched a global strategy to improve women and children's health that relied heavily on the use of mobile devices.

Donors including national aid agencies, international institutions, and philanthropic foundations in both the developing and developed worlds have provided tens of millions of dollars for mHealth and electronic health (eHealth) initiatives.[7] According to a report by the World Bank, such commitments appear to be increasing, including a $200 million commitment from Johnson & Johnson for a five-year program targeting expectant and new mothers in developing countries, a significant portion of which will be focused on a program called Mobile Health for Mothers.[8] Developed country funding has also grown significantly, with an estimated $233

5 The World Health Organization, mHealth: New horizons for health through mobile technologies (2011), at **http://www.who.int/goe/publications/goe_mhealth_web.pdf**.

6 *Id.*

7 Christine Zhenwei Qiang, Masatake Yamamichi, Vicky Hausman, Robin Miller, and Daniel Altman, ICT Sector Unit at World Bank, Mobile Applications for the Health Sector, available at **http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/mHealth_report.pdf** (Apr. 2012).

8 Christine Zhenwei Qiang, Masatake Yamamichi, Vicky Hausman, Robin Miller, and Daniel Altman, ICT Sector Unit at World Bank, *Mobile Applications for the Health Sector*, available at **http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/mHealth_report.pdf** (Apr. 2012).

million of venture capital funding for startups in the United States.[9] Indeed, after $86 million was raised in an initial public offering by Epocrates—the most popular medical application used by U.S. healthcare professionals—it was said that mobile applications for healthcare may be the next big trend for venture capital investments.[10]

With the potential that it holds, mHealth has received significant attention in recent years with specific initiatives deployed to study factors that could improve its uptake and effectiveness. One of the areas identified as essential to the broader uptake of mHealth is the need to strengthen mHealth privacy and security and the public's perception of the same – particularly in low- and middle-income countries – the theory being that greater trust in mHealth's privacy and security will encourage more people to use mHealth and benefit from its advantages. However, as will be shown throughout this paper, data privacy and security are affected by a myriad of factors. They are best understood as part of a diverse ecosystem that can strengthen or weaken them in complex ways. Law is only one of those factors but an important one. Law is often seen as a method of effecting behavioral change, creating minimum standards of quality and care, and encouraging broad adoption of recognized best practices. For this reason, the law and regulation of mHealth privacy and security is of special interest to the mHealth community. It is viewed as an essential pillar in building a mature mHealth marketplace. To that end, while remaining

9 Christine Zhenwei Qiang, Masatake Yamamichi, Vicky Hausman, Robin Miller, and Daniel Altman, ICT Sector Unit at World Bank, *Mobile Applications for the Health Sector*, available at **http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/mHealth_report.pdf** (Apr. 2012).

10 Christine Zhenwei Qiang, Masatake Yamamichi, Vicky Hausman, Robin Miller, and Daniel Altman, ICT Sector Unit at World Bank, *Mobile Applications for the Health Sector*, available at **http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/mHealth_report.pdf** (Apr. 2012).

mindful of the law's place in the broader mHealth ecosystem, this paper will provide an overview of the state of mHealth privacy and security laws today, with a closer look at a select group of jurisdictions in Africa, Asia and Latin America, and lay out a framework for further analysis of mHealth privacy and security law issues as mHealth continues to grow and mature.

OBJECTIVE

This paper aims to develop a functional framework for addressing privacy law issues in the mHealth arena worldwide. The framework can be applied to analyze existing privacy law systems and proposals for new privacy laws and regulation. It also lays the groundwork for additional research and analysis of the privacy law issues affecting the uptake of mHealth. The framework reflects and takes into account the international legal and regulatory landscape, cultural conventions, and technological functionalities relating to data security, while maintaining the integrity of patient autonomy as to privacy and confidentiality and the utility of reliable and expedient access to accurate and comprehensive healthcare data by various stakeholders.

BACKGROUND

Dozens of papers and studies have been published in recent years regarding the growth and potential of mHealth. These reports recognize that mHealth continues to be in its nascent state and are keen to point out areas for concerted effort to help mHealth grow in a healthy, robust manner. One of the themes that has emerged from such work is the need to better address the data privacy and security concerns surrounding the use of mHealth.

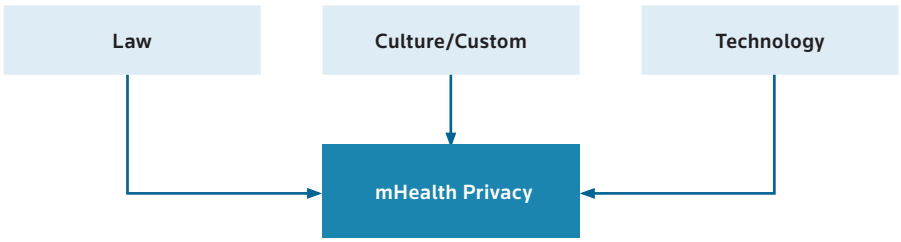
The WHO, for example, has observed that "Data security is a particularly important issue to address within the area of policy.... Policy-makers and programme managers need to be made aware of security issues in the mHealth domain so appropriate policies and strategies can be developed and implemented."[11] The Earth Institute has stated that within the various mHealth policies being discussed, "issues such as data security, access control, and

11 The World Health Organization, *mHealth: New horizons for health through mobile technologies* (2011), at **http://www.who.int/goe/publications/goe_mhealth_web.pdf**.

thus confidentiality must be addressed (as they have been for mFinance).[12] "Questions surrounding the rights to health information should be addressed under this policy framework, in addition to issues regarding information usage."[13] The Association for Computing Machinery published a paper on mHealth privacy from the technologist's perspective that specifically cites the need for policymakers to "establish laws, regulations, and standards regarding the protection of patient privacy in mHealth technology."[14]

Although the need for greater transparency and predictability as to mHealth privacy appears to be broadly recognized and, within that need, a role for policymakers and the law, defining what privacy, security and confidentiality mean in different parts of the world is a challenge. Consequently defining a legal system to address mHealth privacy and security issues in a global sense is challenging. These concepts are influenced by a multitude of factors, including law, technology and custom, among others, that vary widely around the globe.

Figure 1. Mobile Health Privacy Intersects with Law, Technology, Culture/ Custom and Various Other Factors



As such, any privacy law system likely will need to be uniquely adapted to its local environment (its culture, infrastructure, institutions, sophistication, complexity, resources, etc.) despite the inherently global nature of mHealth services and products.

12 Earth Institute. (2010 March). *Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: A Policy White Paper.* mHealth Alliance. Retrieved from **http://cghed.ei.columbia.edu/sitefiles/file/mHealthBarriersWhitePaperFINAL.pdf** (summarizing results from a number of mHealth studies and finding: "The need for security and privacy of data was noted in many studies, and measures such as encryption of data and hardware passwords were used to overcome this barrier. However, given the scope of data collection using mobile phones, guidelines outlining confidentiality protocols need to be developed and the adoption of encryption systems used in mBanking should be considered for mHealth.").

13 Earth Institute. (2010 March). *Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: A Policy White Paper.* mHealth Alliance. Retrieved from **http://cghed.ei.columbia.edu/sitefiles/file/mHealthBarriersWhitePaperFINAL.pdf**.

14 Avancha, S., Baxi, A., & Kotz, D. (2013 March). Privacy in Mobile Technology for Personal Healthcare. Accepted for Publication. ACM Computing Surveys, 45(1). Retrieved from **http://www.cs.dartmouth.edu/~dfk/papers/avancha-survey.pdf**.

Figure 2. Scenarios Illustrating Diversity of Privacy, Security, and Confidentiality Issues[15]

CLUSTER	SCENARIOS AND RELATED ISSUES
NATURE OF PROTECTED DATA	Personal information versus aggregated data; exceptions for law enforcement; public health monitoring; corroboration of end-of-life determinations and surrogate/proxy designations; health research; analysis of health needs for funding decisions; anonymous data could be converted into personal information in countries where a national SIM card registry is maintained; reporting abusive behaviors and violations of rights (Eg. GBV)
COVERED PERSONS/ENTITIES	"Task shifting" of physician and nursing duties to community health workers; scope of liability for private sector hardware and software providers; prevalence of midwifery specialists in developing countries, formal recognition in the United States by the American Nurses Association of nursing informatics as a specialty that combines nursing science, computer science, and information science; individuals reporting abuse; asserting accountability of the health system ("whistle-blowers"?)
SCOPE OF PROTECTED POPULATIONS	Gradations of protection based on disease, minors, gender, legal standing (e.g. whistle-blowers) etc.; cultural expectations relating to privacy regarding sexual and reproductive health, sexual assault or domestic violence, and reporting of inadequacies in the health system
RIGHTS OF NON-PATIENT PERSONS TO ACCESS PROTECTED DATA	Parents, husbands, mothers-in-law, children, same-sex partners, etc., along with cultural perceptions of individual patient's right to privacy with respect to these other parties. Governments? Health authorities?
DATA TRANSFERS	Transfer of data to foreign country server, especially considering prevalence of cloud-based mHealth solutions; Transfers to health authorities (patient-level data vs. aggregate data)
NORMATIVE CULTURAL DISPARITIES	Disparate concepts of privacy, confidentiality, and security, including across urban and rural areas

That being said it will be useful for purposes of this paper to think of mHealth privacy in a broad sense as the ability of all patients to exercise control over the collection, recording, access and dissemination of their mHealth data,[16] such that preserving that ability (in all its subtle variations) should be a priority for those seeking to bring mHealth to scale. mHealth data security can be viewed as a subset of this basic principle and as a necessary ingredient to ensuring that patients can maintain the privacy they seek. Without appropriate physical, technological and administrative security safeguards, all the privacy promises in the world hold limited value. Confidentiality is a related principle and refers to the obligations of those persons who receive mHealth data to preserve its secrecy and use it only as instructed by the patient and/or as necessary to provide the

15 Scenarios developed in cooperation with the mHealth Alliance.

16 Adapted from the definition of "health informational privacy" used by the National Committee of Vital and Health Statistics, a committee within the U.S. Department of Health and Human Services.

services for which the patient entrusted the information to this person. Think of it as the oldest and most low-tech method of ensuring patient privacy.

> CONFIDENTIALITY VS. PRIVACY
>
> Think of "confidentiality" as the oldest and most low-tech method of ensuring patient privacy.

With those general concepts in mind, we will now review in more detail some of the major factors affecting mHealth privacy and security, with some specific examples, to better understand the context for the development of any legal reform in this area.

TECHNOLOGY'S EFFECTS ON MHEALTH PRIVACY AND SECURITY

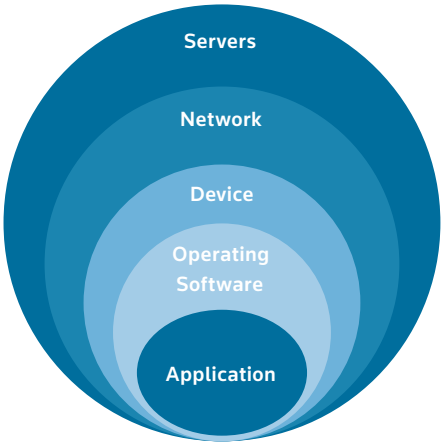
Technology's expansion is mHealth's prime enabler and precisely what makes it suitable for leveraging in even the most remote areas of the globe. But, with all the promise and potential of technology also come various challenges. First and foremost, its ever-evolving nature makes it difficult (and some may say ill-advised) to create rigid legal rules that may not fit future mHealth applications or, worse, that may hamper their development in the first place. Other challenges posed by technology include: absence of cross-border interoperable functionality or standards (e.g., GSM versus CDMA); variety of devices and mHealth technologies (e.g., digital imaging, robotics, micro- and nanotechnologies, genomics); and risks of use (e.g., loss, theft, unauthorized access, malware, cloning, phishing, sharing of devices, lack of understanding about residual availability of data after purported deletions when recycling or discarding, network congestion, etc.).

Technology is also in many ways the first line of defense in terms of providing security to the data that is meant to be kept private. The law may prescribe "reasonable security standards" or require that any such standards are extended by contract to all parties in the data supply chain but the law can seldom set forth with much success the particular technological tools to be applied to fulfill a given legal obligation. In terms of data security especially, the threat is constantly evolving and out-pacing current security standards. A nimble, agile response is required, which detailed regulation can sometimes hamper. Also national detailed data security legislation could create conflicts among laws of different countries where an mHealth application is going to be launched. Developers already struggle with interoperability across borders. Some of the hardest security challenges are the ones that developers face when trying to

deploy their applications on all the networks around the world.[17] Adding a layer of conflicting security regulations to the mix will not help matters.

It is also important to understand that mobile security is itself a layered issue. There is security at the level of the application, the mobile operating software, the hardware device, the wireless network and the wireless carrier, not to mention the servers that transmit, process and store the data and the security practices of the mobile phone users themselves (e.g., setting strong passwords, storing the phone securely). Deciding where to place the obligation to maintain adequate security is a complex question. There are security options available at each of the layers shown below, including secure networks for transmission of data at the server and network level, encryption and password-protection at the device level, firewalls and access controls at the operating software level and secure transmission and limited access to other functions of the mobile device at the application level.[18]

Figure 3. Layers of Mobile Phone Security



CULTURE'S EFFECT ON mHEALTH PRIVACY AND SECURITY

Culture is perhaps the most complex of the major factors affecting mHealth privacy and security. The law, in general, is culturally-specific. Crimes, for example, are defined in vastly different ways across the globe (e.g., in some places jaywalking is a crime, in others adultery by women only is prosecuted criminally). Privacy is particularly culturally sensitive and subjective, so that any legal reform in this area should be adapted to the cultural context in which the laws are to be implemented.

17 Dwivedi, H., Clark, C., & Thiel, D. (2010). *Mobile Application Security*. Retrieved from **http://noorasec.com/books/Mobile_Application_Security.pdf**.

18 For a detailed discussion of mobile security at every level of the mobile ecosystem, see Dwivedi, H., Clark, C., & Thiel, D. (2010). *Mobile Application Security*. Retrieved from **http://noorasec.com/books/Mobile_Application_Security.pdf**.

For example, individual consent is possibly a luxury that is not afforded to individuals in some environments where access may be limited, or even provided through another individual (e.g., in some contexts, women may not access healthcare when it is provided by men, so husbands and fathers will go to the health clinics on behalf of women[19]). Consent in the privacy context, thus, would have to take into account what legal and practical capacity to consent exists for the individuals concerned. This is a nearly-universal issue when it comes to consent by children and, in some places, can also be an issue for women or marginalized populations. In Indonesia, for example, there are practices of mandatory pregnancy tests, virginity tests, and a number of laws and practices that deny Indonesian women who become pregnant outside marriage full access to maternal care and reproductive health.[20] These practices could also have repercussions in terms of who is deemed to have access to the results of such tests.

In a more practical sense, the developed world model of personal ownership of a phone may not be appropriate as the sole model in the developing world where shared mobile telephone use could be common (although perhaps decreasingly so).[21] The mHealth community should be sensitive to the use of shared mobile phones and the effect such practices have on the concept of privacy and individual consent. Of course, for some types of health information, such as a preloaded generic first aid information kit, there would be less concern, while for others more sensitive and personal information, especially personal medical records and targeted SMS messaging for conditions that may be stigmatized such as HIV/AIDS, shared mobile phones could pose a real challenge to the preservation of patient privacy and confidentiality.[22]

LAW'S EFFECT ON mHEALTH PRIVACY AND SECURITY

In countries where privacy (also known as data protection) laws have been enacted and then vigorously enforced, there is generally broader awareness of privacy rights and greater consistency in the level of privacy disclosures made to individuals before they are asked to provide personal information. Failure to provide these disclosures and/or abide by the privacy promises made in these disclosures can lead to quite severe administrative fines and penalties and, in some places, even civil causes of action with both compensatory and punitive damages. As will be set forth in greater detail below, even among

19 Policy Engagement Network for the International Development Research Centre. (2010 December). *Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations*. The London School of Economics and Political Science. Retrieved from **http://personal.lse.ac.uk/martinak/eHealth.pdf**.

20 Policy Engagement Network for the International Development Research Centre. (2010 December). *Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations*. The London School of Economics and Political Science. Retrieved from **http://personal.lse.ac.uk/martinak/eHealth.pdf**.

21 Earth Institute. (2010 March). *Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: A Policy White Paper.* mHealth Alliance. Retrieved from **http://cghed.ei.columbia.edu/sitefiles/file/mHealthBarriersWhitePaperFINAL.pdf**

22 Earth Institute. (2010 March). *Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: A Policy White Paper.* mHealth Alliance. Retrieved from **http://cghed.ei.columbia.edu/sitefiles/file/mHealthBarriersWhitePaperFINAL.pdf**

these countries with actively enforced privacy laws, they take vastly different approaches to regulating privacy. These different approaches lead to different methods (and related costs) of compliance but it is more difficult to ascertain the differing results in terms of achieving the goal of giving individuals the ability to exercise control over the collection, recording, access and dissemination of their personal information. It is also difficult (although less so) to assess the true compliance cost of certain approaches, both in terms of actual costs of compliance (implementation, legal advice, required changes to process or business model) and the more abstract costs to innovation and diverse investment in the regulated sector. For this reason, rather than advocating for the adoption of a particular approach, this paper aims to provide an overview of the different approaches and bring these laws down to their elements so that a functional privacy law framework can be developed.

In addressing the effect of law on mHealth privacy and security, one must also be conscious of the effect of non-privacy laws. For example, many countries are now mandating national SIM card registries, so that every mobile phone can be linked back to an individual citizen.[23] In such countries, any definition of personal information may need to take into account that at least certain government agencies would be able to de-anonymize information transmitted over mobile phones and, thus, turn it into personal information. Protections could also be put in place to limit the government's ability to share this information across agencies or use it for law enforcement purposes.

GENDER-BASED PRIVACY CONCERNS

There are countries where adultery is a criminal offense for women, so that innocent or inadvertent release of such information to third parties (including family members) could lead to severe punishment of the patient.

In another type of example, the laws that apply to women in some countries can make a mobile-enabled diagnosis into a very serious legal offense. For instance, the diagnosis of a recessive genetic disorder can also inadvertently reveal non-paternity if the father and child are both tested (a recessive disorder requires the disease causing mutation to be present in both parents and for the child to inherit both copies).[24] There are countries where adultery is a criminal

23 For example, SIM card registration in Uganda is part of the East Africa Communications Organisation (EACO) initiative, which set mid 2012 as the deadline to have all existing SIM cards in East Africa registered. In Kenya and Tanzania at least 80% of SIM cards in each country have been registered. Republic of Uganda, Ministry of Communications and Information Tech., **http://www.ict.go.ug/index.php?option=com_content&view=article&id=153:sim-card-registration&catid=36:other-news**

24 Scenario comes from Policy Engagement Network for the International Development Research Centre. (2010 December). *Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations*. The London School of Economics and Political Science. Retrieved from **http://personal.lse.ac.uk/martinak/eHealth.pdf**.

offense for women, so that innocent or inadvertent release of such information to third parties (including family members) could lead to severe punishment of the patient. In such countries, where disclosure of certain types of mHealth data could lead to severe consequences under seemingly unrelated laws, perhaps the punishment for even inadvertent disclosures (absent of bad faith) contrary to patient instructions or the promises made by the mHealth provider should be especially severe to effectively deter such conduct and encourage sufficient safeguards to prevent these unintended repercussions. A corollary revision to the laws of evidence to exclude the admissibility of such personal information to prove adultery could also be introduced but this type of provision would be less likely to be enacted where the laws are particularly aggressive in the prosecution of these types of offenses against women.

OTHER FACTORS AFFECTING mHEALTH PRIVACY AND SECURITY

Technology, culture and the law are only a few of the most visible factors affecting mHealth privacy and security. Countless other less obvious factors interact with both the conception of privacy and security and the ability to effect any change in these areas. Any reform to privacy and security law should take special care to identify all such factors, especially those with greater impact where an exhaustive list is not pragmatic, and assess them as a system with multi-lateral cause and effect scenarios that can have repercussions many layers away in the mHealth ecosystem.

A recent study from the London School of Economics pointed out that this issue is even more acute in resource-constrained environments, such as low-income countries and disaster-relief situations (where mHealth could be leveraged to even greater effect):

> "Neither the patients nor the practitioners are particularly aware of rights and responsibilities. Literacy may be minimal, so notices are insufficient. Populations may be more mobile and therefore patient registration may be even more important and yet difficult to achieve. Care providers may be responsible for larger numbers of patients. Staff may not be trained in procedures. The technical infrastructure may vary, with problems with electricity, so running additional processes and procedures may prove too challenging. Multiple organizations may be operating in the same space, with implementing partners and government agencies, whereby it may be difficult to identify the primary custodians of the information. All of these barriers are exacerbated in humanitarian operations."[25]

25 Policy Engagement Network for the International Development Research Centre. (2010 December). *Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations*. The London School of Economics and Political Science.Retrieved from **http://personal.lse.ac.uk/martinak/eHealth.pdf**.

In such situations, flexibility and adaptability of privacy regulation or the adoption of certain safe harbors may be particularly important as rigid rules may cause users to abandon mHealth altogether for inability or impracticability of complying weighed against the high need for the medical services being sought. Indeed, the same data security regulations employed in the United States with some success may be of no use to a low-income country with fewer enforcement capabilities and less-developed infrastructure. Any solution must be adapted to its unique environment.

LACK OF AWARENESS OF PRIVACY RIGHTS A CHALLENGE IN RESOURCE-CONSTRAINED ENVIRONMENTS

"Neither the patients nor the practitioners are particularly aware of rights and responsibilities. Literacy may be minimal, so notices are insufficient. Populations may be more mobile and therefore patient registration may be even more important and yet difficult to achieve."

In addition, it is important to consider what industry efforts are being made to increase the privacy and security of mHealth. Such initiatives could address a number of key concerns in an effective and flexible manner and any legal reform should take stock of these initiatives to both learn from them and to ensure that any new laws or regulations do not negatively impact any positive aspects of such programs. For example, in January 2011, the GSM Association published a set of universal Mobile Privacy Principles that describe the way in which mobile consumers' privacy should be respected and protected when consumers use mobile applications and services that access, collect and use personal information.[26] In collaboration with representatives from the mobile ecosystem, the GSM Association has also developed a discussion document outlining a set of Privacy Design Guidelines for Mobile Application Development. These documents are geared toward the privacy of personal information generally, not mHealth specifically, but are indicative of the type of industry efforts aimed at addressing privacy from the earliest stages of design and development.

USES OF MHEALTH AND THE "mHEALTH ECOSYSTEM"

Crucial to developing an adequate mHealth privacy and security framework (while acknowledging the roles of technology, law, custom and other factors) is understanding how mHealth data flows and is used (and by whom). Any privacy solution must make sense given mHealth's current and potential uses and applications.

26 Available at **http://www.gsma.com/publicpolicy/mobile-and-privacy/gsma-mobile-privacy-initiative**.

mHealth Uses

A recent study conducted by PricewaterhouseCoopers and funded by the GSM Association estimates that the worldwide mHealth market will grow to approximately $23 billion by 2017.[27] This market contains applications ranging from wellness and diet to diagnosis and treatment. Europe leads the way, with the United States close behind and then Asia, Latin America and Africa. Although Africa still lags behind its neighbors in mHealth adoption, news reports show that, where used, mHealth is being successfully deployed in several African countries.[28] Tanzania, for example, uses mobile stock management technology to track malaria treatments in 5,000 clinics across the country.[29] In South Africa, 1,800 remote community health workers use mobile phones to access and update patient records. And when Ghana rolled out rotavirus and pneumococcal vaccines this April, a major local religious organization helped notify mothers about the new immunizations by arranging for 1.5 million SMS messages to be sent out.[30] South Sudan, supported by the WHO, began to manage vaccine stocks through mobile technology in mid-2012 in its central and state stores, while Rwanda's health ministry uses mobile phones to monitor maternal and child mortality.[31] Other uses for mHealth include:

- Enumeration of clients and service equity (patient registration & vital events tracking)
- Continuity of care (electronic health records)
- Accountability for health services (scheduling & reminders)
- Increased safety and quality of care (decision support for providers)
- Knowledge and access to information (education & behavior change communication)
- Skilled health workforce (providing training and service updates)
- Access to commodities & health staff (commodity & human resources management)
- Reduce financial & motivational barriers (health financing & incentives)
- Connected health system (communication & telemedicine)
- Up-to-date national health information (real-time indicator reporting)[32]

---

27 GSM Association, Touching Lives Through Mobile Health: An Assessment of the Global Market Opportunity, available at **http://www.pwc.in/assets/pdfs/telecom/gsma-pwc_mhealth_report.pdf** (Feb. 2012).

28 Kristin Palitza, Inter Press Service News Agency, Africa's Mobile Health Revolution (Dec. 22, 2012), available at **http://www.ipsnews.net/2012/12/africas-mobile-health-revolution/**.

29 Kristin Palitza, Inter Press Service News Agency, Africa's Mobile Health Revolution (Dec. 22, 2012), available at **http://www.ipsnews.net/2012/12/africas-mobile-health-revolution/**.

30 Kristin Palitza, Inter Press Service News Agency, Africa's Mobile Health Revolution (Dec. 22, 2012), available at **http://www.ipsnews.net/2012/12/africas-mobile-health-revolution/**.

31 Kristin Palitza, Inter Press Service News Agency, Africa's Mobile Health Revolution (Dec. 22, 2012), available at **http://www.ipsnews.net/2012/12/africas-mobile-health-revolution/**.

32 Adapted from the "WHO mHealth Framework for RMNCH", available at **https://www.hl7.org/documentcenter/public_temp_72547FD3-1C23-BA17-0C406ABE0F78EA5E/wg/mobile/WHOmHealthFrameworkforRMNCHDescription.pdf**.

These different uses will trigger subtle differences in how patients seek control over the collection, recording, access and dissemination of their mHealth data. For example, in a text messaging campaign to increase adherence to antiretroviral treatment, patients noted that it was important to them that the messages maintained confidentiality and privacy by using coded words or phrases ("Remember, it is the time of your life") instead of "sensitive" words (HIV or antiretroviral), suggesting that patients want health-related SMSs that appropriately notify them, deliver a carefully crafted message, and are sensitive to the context in which they are received.[33] These are relatively common sense (though not self-evident) methods for ensuring privacy of mHealth data that legal regulation would have little ability to prescribe. A combination of user-centric design by mHealth providers and developers must factor into the contemplated privacy solutions to ensure greater effectiveness. This example shows that law alone cannot always identify the best practice in a given situation that is sufficiently well-suited to the particular patient.

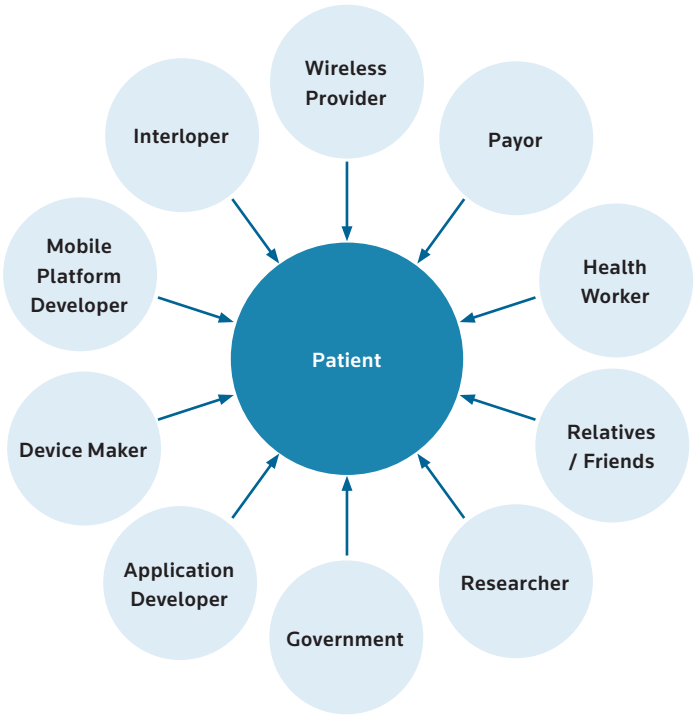
By the same token, the level of security mechanisms that would be appropriate to protect a phone with an attached monitoring device that stores mHealth data locally and remits it to a health care provider remotely should be as sophisticated as the device itself. Mandating this same level of security, likely including encryption and other high-technology solutions, on the HIV treatment text-messaging campaign described above would not be effective and would do nothing to protect the privacy of the information transmitted across the device if it still spoke in plain terms about the HIV treatment instead of using coded language. In sum, there is no one-size-fits-all solution.

mHealth Stakeholders

We have already mentioned the importance of patients and ensuring patients' autonomy as to how their mHealth data is handled, but there are other participants in the mHealth ecosystem to consider as well, all of whom may contribute to a patient's mHealth data record, maintain it, access it or use it in varying ways that should inform the development of any new privacy laws and regulations. As this system matures, more and more of these information transfers may occur between information exchanges to which all the participants may have access.

33 Earth Institute. (2010 March). *Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: A Policy White Paper.* mHealth Alliance. Retrieved from **http://cghed.ei.columbia.edu/sitefiles/file/mHealthBarriersWhitePaperFINAL.pdf**.

Figure 4. The mHealth Ecosystem Comprises Multiple Actors with Access to Patient Data



METHODOLOGY

Based on the background set forth above and the resulting sketch of the "mHealth ecosystem", this paper analyzes current research on mHealth privacy issues and provides a broad overview of the current global landscape of national policies, laws and regulations that target privacy and security issues as they relate to mHealth. The resources relied upon for this part of the paper include original laws, academic commentary, judicial interpretation and regulatory guidance from selected representative countries from North America, Europe, Africa, Latin America and Asia. The result of this research is a global mHealth privacy law landscape, highlighting regional variances in approach to privacy law in an attempt to showcase the options available as the mHealth community continues to grapple with how best to strengthen mHealth privacy and security through the law.

The second section of the paper takes a closer look at the state of privacy law and any particular legislation and policy in the mHealth space in a select group of jurisdictions by conducting a high level gap analysis in consultation with local privacy attorneys in Tanzania, Uganda, Nigeria, Bangladesh, India, Peru and Chile, jurisdictions that have begun to experience promising mobile health programs. The results of this analysis are summarized and identifiable trends are highlighted.

Finally, informed by the above analyses and research, this paper sets out to create a functional privacy law framework that can be applied to different scenarios and environments to produce a thoughtful discussion and drive toward the over-arching guiding principle of providing patients control and autonomy over their mHealth data while preserving the efficacy of mHealth solutions and applications.

Please note that this paper is not intended to provide a comprehensive digest of all applicable laws of any jurisdiction surveyed or reviewed, nor does it encompass review of or recommendations about technological functionalities relating to data storage, processing, or transmission.

GLOBAL LANDSCAPE OF CURRENT mHEALTH PRIVACY AND SECURITY LAWS AND PATIENT CONFIDENTIALITY

LAWS

This section provides a high-level summary of the most pertinent laws from a number of representative jurisdictions across the globe, followed by a description of the main elements of each law (e.g., covered entities, covered data, disclosure obligations, penalties, etc.). The aim is to provide the mHealth community with an inventory of the health privacy laws on the books, so that different approaches can be analyzed and new approaches may be contemplated. Although organizations such as the WHO have conducted global surveys of laws directly related to eHealth,[34] these reports do not go into detail with respect to specific legal provisions contained in the existing laws that do or might impact eHealth and/or mHealth.

Also, unlike the WHO surveys, this overview does not take a position as to whether one legal approach is superior to another or whether any existing laws are insufficient to address the new challenges posed by eHealth and mHealth. This section merely aims to provide a compilation of current representative laws for further study and analysis by the mHealth community according to the framework developed in this paper.

The laws and approaches discussed in this section differ significantly, but we have broken down each law into the following core elements to aid comparison and the learning process:

- Coverage
  - Persons/entities obligated to comply
  - Personal information covered
  - Scope of coverage
- Information/Notification requirements
  - Consent requirements

34 World Health Organization, Legal Frameworks for eHealth (2012), available at **http://www.who.int/goe/publications/ehealth_series_vol5/en/**.

- Data security obligations
  - Retention/Destruction
  - Technical and organizational security (including cloud storage)
  - Breach notification obligations
- Data transfer (including cross-border) requirements
- Enforcement and sanctions

None of the laws reviewed and none known to the authors to date explicitly address mHealth. However, some laws regulate health privacy (and some even expressly address electronic health privacy) specifically and do so sufficiently broadly so as to arguably reach mHealth applications if such applications were to handle covered data (i.e., remote diagnostic services would likely be covered while general health information applications would not due to the scope of many applicable laws). Others have no specific health privacy regulations but cover all types of personal information equally, so that mHealth applications that handle covered data (relating to an identifiable person) would also be subject to these laws.

Some countries in Latin America, Asia, and Africa without comprehensive privacy laws or specific health privacy laws do have constitutional protections and/or medical ethics codes to provide some level of protection. However, these countries are facing a choice as to whether to implement new laws (as Mexico and Singapore have recently done) and, if so, whether to adopt a sectoral approach (with laws specific to certain industries or sectors, such as in the United States) or an omnibus approach (with one national law covering all types of personal information and imposing a minimum level of regulation across all types of data). Then, they must decide where to draw the line on scope of coverage, level of regulatory detail, and enforcement mechanisms. For these countries, this section can provide a roadmap for different types of options.

Countries with existing laws face the constant question of whether to continue to legislate and for what purpose. For these countries, this section can provide a general sense as to what other countries are doing and what level of regulatory rigor they are applying. We begin our review with the United States, which has one of the most-detailed health and eHealth privacy statutes currently on the books. We then review the competing European omnibus approach and examples of legislation currently in force in Latin America, Asia, and Africa. As noted above, however, we have not included in this section an assessment as to which approach is better in part because we believe the answer will depend on the local context and capabilities.

NORTH AMERICA

UNITED STATES

U.S. PRIVACY IN BRIEF

- No overarching privacy law
- Emphasizes that mobile app developers should provide clear, readily-identifiable and easy to understand methods to notify a user when certain kinds of data are being collected and/or transmitted
- Laws generally require that organizations maintain "reasonable security" over personal data, taking into consideration the sensitivity of the data that is collected and stored

Introduction to Applicable Laws

The United States, unlike many other countries, does not have an overarching data privacy law that applies to all types of personal information, including health information. However, it does have a general health privacy law with broad application that may be extended to mHealth to the extent the data concerned fits the legal definition of covered data (denoted as "protected health information" in this particular law) and the entities involved in the processing of data qualify as a "covered entity" (or a business associate/service provider of such covered entity). In addition, there is a patchwork of federal and state laws that regulates particular kinds of data and industry sectors, which may be extended to mHealth as well.

Federal Laws

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA")

One of the most important federal laws governing confidential health information in the United States is the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[35]

Pursuant to HIPAA, the U.S. Department of Health and Human Services ("HHS") has issued regulations governing the privacy of health information that is maintained in electronic form, notably the "Privacy Rule" and the "Security

35 Pub. L. No. 104-191, as implemented by 45 C.F.R. § 160, 162, 164.

Rule." The Privacy Rule requires that certain entities, including health plans and healthcare providers who transmit health information, ensure the confidentiality of certain health-related information. These entities cannot disclose health information except for purposes of treatment, payment for treatment, and health care operations without obtaining authorization from the patient or participant. The Privacy Rule also affords patients and participants certain rights with respect to their data, such as the right to access and suggest changes to records of their health information and to be informed of certain disclosures of their health information to others. The covered entity must also comply with certain administrative requirements, such as providing notices to patients and participants about how the entity handles their health information.

The Security Rule provides certain technical and organizational requirements so that covered entities "[e]nsure the confidentiality, integrity and availability"[36] of health information. The Security Rule outlines various obligations to ensure this goal, including appointing and training certain employees regarding security, establishing certain plans to identify and respond to risks such as interference with system operations and unauthorized access, use, disclosure or modification or data, and establishing procedures to ensure that only authorized individuals have access to health information.

In addition, the "Business Associate" rules require that covered entities enter into agreements with other entities that perform functions for the covered entity where the third party may have access to health information. Pursuant to the HITECH Act (as further described below), these third parties, or "business associates" may be subject to direct government enforcement and may incur penalties for violating HIPAA rules.

In 2009, another law was passed (the "HITECH Act") that revised the Privacy Rule and the Security Rule. The final omnibus rule pursuant to these revisions was published by HHS on January 25, 2013.[37] In particular, the new omnibus rule expands the entities covered by HIPAA to include Health Information Organizations, entities that provide data transmission services for health information, and personal health record vendors.

These obligations may require mobile health technology providers to enter into business associate agreements with their own subcontractors that impose the same HIPAA compliance requirements on the subcontractor that apply to the business associate. The new rule also relaxes some limitations on the use of health information for the purpose of fundraising. In addition, the rules prohibit selling health information without authorization, but disclosure for research purposes and certain other purposes are permitted, and it is acceptable to receive a reasonable fee for the cost of preparing and transmitting the health information.

36 45 C.F.R. § 160.103.

37 78 Fed. Reg. 5566.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998 ("COPPA")

The Children's Online Privacy Protection Act of 1998[38], as implemented by the Children's Online Privacy Protection Rule[39] (the "Rule") (collectively "COPPA") prohibits the collection of personal information from children under the age of 13 through commercial websites or online services without obtaining express consent from a parent or legal guardian. This law could apply in the mHealth context to the extent applications collect personal information directly from children. This law also provides an example of how legislators have addressed the difficult task of developing effective authentication procedures (to confirm parental consent), which could be instructive to the mHealth community.

COPPA, as recently amended, may require mobile health technology providers that collect health information from children, such as through pediatric care applications, to establish procedures for obtaining express parental consent for the collection and processing of that information. Such providers would also need to ensure that they provide the proper notices through their mobile applications and maintain reasonable security procedures to protect the data collected. If such mobile healthcare providers use third parties to process personal information collected from children, the providers would also need to require that the third parties maintain security measures to protect the information.

FEDERAL TRADE COMMISSION ACT ("FTC ACT")

Under Section 5 of the Federal Trade Commission Act ("FTC Act")[40], the Federal Trade Commission ("FTC") has broad authority to take action against individuals and/or entities that engage in what the FTC Act terms "unfair or deceptive" practices. Pursuant to this authority, the FTC has taken action against organizations that violate their consumer privacy policies (considered a "deceptive" practice) and, more recently, against organizations that engage in practices that the FTC has deemed to be contrary to consumer protections or otherwise harmful to consumers, even where those practices are disclosed in consumer privacy policies (considered "unfair" practices).

While the FTC Act itself does not set forth express requirements regarding data protection, the FTC has published specific guidance regarding its approach to data protection enforcement under the FTC Act, including the Framework and the Report (the "Guidance").

In February 2013, the FTC issued guidance specifically for mobile applications in a report titled "Mobile Privacy Disclosures: Building Trust Through Transparency." (the "Report"). In the Report, the FTC specifies four primary

38 15 U.S.C. § 6501 et. seq.

39 16 C.F.R. § 312.1 et. seq.

40 15 U.S.C. § 45.

recommendations that mobile app platforms, or interfaces through which consumers access mobile applications, should adopt: (1) consistent disclosures; (2) oversight across apps; (3) transparency regarding mobile app review; and (4) a Do Not Track mechanism for behavioral advertising. For mobile application developers, the Report provides that they should (1) establish and publish a privacy policy for their apps that is available through the platform; and (2) provide just-in-time disclosures and obtain user consent for the collection of "sensitive content" beyond a platform's application programming interface ("API") (but not to overlap with disclosures issued by the platform), among other requirements. Overall, the Report stresses the need for mobile application platforms and developers to provide clear, readily-identifiable, and easy to understand methods to notify a user when certain kinds of data are being collected and/or transmitted.

State Laws

STATE BREACH NOTIFICATION LAWS, INFORMATION SECURITY REQUIREMENTS AND SENSITIVE INFORMATION RESTRICTIONS

Many individual U.S. states have enacted their own information security and breach notification laws that require organizations to implement security measures to protect certain types of personal data and provide notice in the event of a data security breach affecting certain types of personal data.

As of January 2013, forty-six states, the District of Colombia, Puerto Rico, and the Virgin Islands have all enacted some form of a breach notification law[41]. These laws generally require an individual or an entity that "owns or maintains" certain types of personal information about a state resident to notify that resident and possibly state agencies, credit reporting agencies, and the media in the event of a data security breach. The laws typically set forth requirements around the timing, format, and content of the notice, which vary by state.

In addition, an increasing number of U.S. states have enacted information security laws that require covered individuals or legal entities that process certain types of personal information to implement information security measures to protect the security and integrity of that information. The specific elements of the required security measures typically vary by state. In general, however, state information security laws require covered entities to implement "reasonable" security measures, appropriate to the type of personal information. The Massachusetts information security law, however, differs from most other such state laws. Instead of setting forth a reasonableness standard, the Massachusetts law requires covered individuals and entities to implement specific administrative, physical, and technical safeguards on a comprehensive

41 As of January 2013, Alabama, Kentucky, New Mexico, and South Dakota have not enacted breach notification laws.

level. Massachusetts has adopted specific regulations that set forth the elements of those safeguards (the "Regulations").

As applied to mobile health technology providers, state breach notification laws would require such providers to issue notice to affected individual residents of a state with such a law if the provider holds personal information about state residents that is covered under and accessed in a manner that triggers the relevant law. A limited number of U.S. states (e.g., Arkansas, California, Missouri, Texas, and Virginia) include health and/or medical data within the types of data covered by security breach notification laws. In those states and well as under HIPAA (for covered entities and business associates) unauthorized loss and/or access to health and medical information would likely trigger breach notification requirements. Additionally, mobile health technology providers would generally be required to implement reasonable security measures to protect individual health and medical data. Where the provider holds covered data about Massachusetts residents, the provider will likely be obligated to implement a comprehensive information security program incorporating the particular elements required under the Massachusetts information security law.

Other Laws

Some additional U.S. laws may potentially apply to the collection and processing of mHealth data. These laws include the Stored Communications Act and the FTC Secure Disposal Rule.

The Stored Communications Act[42] ("SCA") prohibits an entity that provides an electronic communication service ("Service") from knowingly disclosing the contents of a communication that the Service is holding in electronic storage. Disclosure is, however, permitted if the Service obtains express consent for the disclosure from the originator of the communication or the addressee or intended recipient. Penalties for violation of the SCA consist of civil claims for damages. Assuming that mobile health technology providers are deemed to be Services under the SCA, such providers would need to be aware of their disclosures of consumer health and medical data and would need to avoid any knowing disclosures, particularly without consumer consent, in violation of the act.[43]

The FTC Secure Disposal Rule[44] ("Rule") applies to entities that maintain consumer information for business purposes and requires that they properly dispose of that consumer information to protect against unauthorized disclosure. While the Rule does not specify particular disposal procedures that qualify as "proper" disposal under the Rule, it does provide specific examples of proper disposal measures. Pursuant to the Rule, mHealth providers would be

42 18 U.S.C. §§ 2701-2712.

43 The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, also protects wire, oral, and electronic communications while in transit and may have some limited application to mHealth.

44 16 C.F.R. 682.

obligated to implement proper, secure disposal procedures for any individual health and medical information about consumers of mHealth services that they may collect and store.

Coverage of Data Protection Regulation

PERSONS/ENTITIES OBLIGATED TO COMPLY

HIPAA: HIPAA applies to "Covered Entities" under the statute. These include Health Plans, Health Care Clearinghouses, healthcare providers that transmit health information in electronic form, and "business associates" of those covered entities.

COPPA: COPPA applies to "Operators," which includes a person or entity who operates a commercial website or online service that collects or maintains personal information, as defined under the statute, as well as a person or entity who collects personal information on behalf of an Operator.

FTC ACT: According to the FTC Framework, the FTC's authority under the FTC Act applies to nearly all commercial entities that collect consumer data.

STATE LAWS: The applicability of state breach notification laws and information security laws varies by state. In general, these laws apply to any natural person or legal entity that "owns or licenses" personal information of state residents.

COVERED DATA

HIPAA: HIPAA covers "protected health information" or "PHI". Under the statute, PHI includes information that can be used to identify an individual and relates to an individual's past, present or future medical condition, the provision of health care to an individual, and past, present and future payment for the provision of healthcare to the individual. This data can include an individual's name, address, birth date, and Social Security Number. The final omnibus rule addresses the use and disclosure of genetic information.

COPPA: COPPA covers personal information from a child under the age of 13 and includes a broad range of data types, including first and last name, physical address, social security number, persistent identifier, videos, photographs, geolocation information, and information concerning the child or the child's parent or legal guardian that is combined with an identifier.

FTC ACT: Based on the FTC Framework, the FTC's authority pursuant to the FTC Act covers consumer data that can be linked to an individual consumer, as well as data about a specific computer or device (such as cookie data and Unique Device Identifiers ("UDIDs") for mobile devices).

STATE LAWS: Both state information security and breach notification laws generally apply to "personal information", which, on a high-level, consists of

an individual's name combined with other more sensitive data such as: social security number, driver's license number, financial account number, and health or medical data.

SCOPE OF COVERAGE

HIPAA: The statute applies to a covered entity's use and disclosure of PHI.

COPPA: COPPA generally prohibits unfair or deceptive activities related to online, collection, use and/or disclosure of personal information from a child under the age of 13.

FTC ACT: The FTC's authority under the FTC Act applies to data collection and use practices that could be deemed to constitute "unfair" or "deceptive" practices that may adversely impact consumers.

STATE LAWS: State breach notification laws generally apply to individuals and legal entities that "own or maintain" personal information (as defined by the statute and described generally above) about residents of the state.

INFORMATION REQUIREMENTS

HIPAA: The statute requires each covered entity to provide data subjects with a notice describing the entity's privacy practices. HIPAA sets forth specific content requirements for these notices. In particular, the notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must also describe an individual's rights, including the right to complain to the U.S. Department of Health and Human Services and to the covered entity if the individual believes that his or her privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities are obligated to act in accordance with their notices. HIPAA also specifies when and how such notices should be provided to individuals. A covered entity must also provide notice to an individual upon that individual's request. In addition, entities that are covered by HIPAA are required to provide notification to affected individuals and to HHS if the entity discovers a breach of unsecured health information.

COPPA: Under COPPA, an Operator must post a prominent link to a notice regarding the Operator's data collection and use practices on its website's homepage and on any page through which personal information from children may be collected. The statute specifies the types of information that must be included in the notice. An Operator must typically also provide notice directly to a child's parent or legal guardian before it collects personal information.

FTC ACT: In its Guidance, the FTC has called for greater transparency in the collection and use of data. Recently, the FTC has placed a particular emphasis on transparency by mobile applications. As part of promoting transparency,

organizations must issue privacy notices that are clear, conspicuous, and more standardized, especially mobile app developers and platforms. Organizations must also issue prominent disclosures to inform consumers of changes in the organization's use of data and educate consumers about the organization's privacy practices.

STATE LAWS: Generally, state breach notification statutes require that notice be provided to affected individuals, but states vary on the timing, format, and content requirements for the notice. Some states do not specify content requirements, and those that do vary with respect to those requirements.

California's content requirements provide that the notice include, at a minimum: (a) the name and contact information of the reporting person or business; (b) a list of the types of personal information that were or are reasonably believed to have been the subject of the breach; (c) if the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred; (d) the date of the notice; (e) whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; (f) a general description of the breach incident, if that information is possible to determine at the time the notice is provided; and (g) the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

The Massachusetts information security law does not contain notice requirements.

CONSENT REQUIREMENTS

HIPAA: A covered entity must obtain an individual data subject's consent to disclose his or her PHI where disclosure is not otherwise provided for under the statute. In addition, a covered entity in a direct care relationship with an individual is required to make a good faith effort to obtain written acknowledgment from the individual that the individual received the entity's HIPAA notice.

COPPA: Under COPPA, a child cannot validly consent to the collection of his or her information. An Operator must obtain consent from a parent or legal guardian. The Operator is required to make any reasonable effort to ensure that before personal information is collected from a child, a parent or legal guardian (i) receives notice as specified under the statute and (ii) authorizes any collection, use, and/or disclosure of the child's personal information. The Operator must also provide an option to consent to the collection of the child's data without also consenting to the disclosure of that data to a third party. Additionally, the Operator is required to take steps to ensure that the individual providing consent is the child's parent or legal guardian, and the statute specifies acceptable forms

of consent for this purpose. In some specific cases, the Operator may obtain consent after it collects the personal information.

FTC ACT: In its Framework, the FTC requires that organizations provide streamlined choices to consumers regarding the use of consumer data. In particular, the Framework provides that express consent must be obtained for the collection and use of health and medical data. With respect to mobile applications in particular, the Report provides that organizations should provide consumers with just-in-time disclosures and obtain express consent for the collection of "sensitive content". The Report does not clearly define "sensitive content" but states that it includes geolocation data and generally includes data that other countries may identify as "sensitive." Additionally, the Framework requires obtaining consent in the event of material changes in the organization's use of data.

STATE LAWS: Generally, neither state breach notification laws nor state information security laws contain consent requirements. For reference, both the California breach notification law and the Massachusetts information security law do not contain such a requirement.

DATA SECURITY OBLIGATIONS

RETENTION

HIPAA: A covered entity may include particular record retention policies as part of its required security practices. However, HIPAA does not specify a clear time limit on the retention of PHI. HIPAA does require that covered entity retain its privacy policies and procedures, privacy practices notices, disposition of complaints, and other documentation required under HIPAA for six (6) years after their creation or last effective date.

COPPA: COPPA does not provide specific limitations on retention of personal information. However, it does specify that personal information collected in certain circumstances without first obtaining consent must be deleted after it has been used for the purpose for which it was collected. The amendments to the Rule also require that Operators adopt reasonable procedures for data retention and deletion. In addition, the Operator must delete the child's personal information upon a parent or legal guardian's request at any time.

FTC ACT: The Framework provides that organizations must implement reasonable restrictions on the retention and disposal of the data once it is no longer needed for the legitimate purpose for which it was collected. However, the Framework specifies that retention policies should be flexible and related to the type of data retained.

STATE LAWS: State information security laws generally require reasonable security measures to protect personal information. The Massachusetts information security law does not contain express provisions around retention.

SECURITY (INCLUDING CLOUD STORAGE)

HIPAA: A covered entity is required to maintain reasonable and appropriate administrative, technical and physical safeguards to protect PHI from unauthorized use or disclosure. The HIPAA Security Rule sets forth applicable security requirements.

COPPA: An Operator is required to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information that it collects from children.

FTC ACT: The FTC Framework provides that organizations must provide reasonable security to protect consumer data. The Framework also requires reasonable limitations on the collection of information to a level that is consistent with the context of the transaction with the consumer.

STATE LAWS: State information security laws generally require reasonable security measures to protect personal information. The Massachusetts information security law requires that every individual or entity covered by the law develop, implement, maintain, and monitor a comprehensive information security program applicable to any records containing personal information of Massachusetts residents, and the information security program must contain administrative, technical, and physical safeguards to ensure the security and confidentiality of the personal information.

IDENTITY AND AGE VERIFICATION PRACTICES

HIPAA: HIPAA allows for parents to exercise the individual rights of their minor children, as the minor's "personal representatives."

COPPA: As stated, COPPA prohibits collection of personal information from children under the age of 13 and provides steps for confirming the identity of the child's parent or legal guardian for purposes of obtaining consent for the collection and processing of a child's personal information.

FTC ACT: The FTC's authority to enforce COPPA is established under the FTC Act. The FTC Framework also requires reasonable authentication procedures for verifying the identity of consumers seeking to access their data, based on a risk management approach with heightened risks related to sensitive data.

STATE LAWS: The Massachusetts information security law requires secure access control procedures, which could incorporate identity verification for individuals seeking to access their personal information.

BREACH NOTIFICATION OBLIGATIONS

HIPAA: Under the HITECH amendments to HIPAA, a covered entity is required to notify an affected individual in the event of a breach of unsecured PHI. In certain cases, the covered entity must also notify the Secretary of the U.S.

Department of Health and Human Services as well as the media. Notice must be given without unreasonable delay and in no case later than 60 days following discovery of the breach.

COPPA: COPPA does not provide for a specific breach notification obligation.

FTC ACT: The FTC Guidance does not expressly provide for breach notification obligations. However, in practice, an organization could be deemed to violate the data security or transparency obligations under the FTC Framework if it fails to provide notification of a data security breach impacting consumer data.

STATE LAWS: State breach notification laws generally require an individual or legal entity that "owns or maintains" personal information, as defined by the particular statute, to notify impacted individuals of any data security breach, which generally consists of any unauthorized access or acquisition of such personal information that is unencrypted. As noted in other sections of this summary, the timing, format, and content requirements of the notice vary by state.

DATA TRANSFERS (INCLUDING CROSS-BORDER)

HIPAA: HIPAA does not expressly require notice or consent upon data transfer. However, in general, if such a transfer is related to or necessary to complete one of the purposes for which disclosure is permitted under the statute, the covered entity may engage in that transfer. Where the statute does not provide grounds for such a transfer, the covered entity will be required to obtain the written authorization of the individual for the underlying disclosure to which the transfer is related.

COPPA: COPPA does not expressly require consent or impose restrictions on data transfer. However, an Operator must state in the required notice whether any personal information is transferred to third parties, the types of business engaged in by the third parties, the purposes for which the personal information is used by the third parties, and whether the third parties are subject to an agreement to maintain the confidentiality, security and integrity of the personal information that they receive.

FTC ACT: The FTC Framework requires that organizations disclose third party recipients of consumer data as part of their adherence to the transparency principle. In addition, the FTC Report provides that mobile app developers should consider using icons to indicate when data is being transferred.

STATE LAWS: State breach notification and information security laws do not generally contain express requirements for notice or consent upon data transfer. In general, however, covered entities must comply with the requirements of the state breach notification and information security laws even where personal information has been transferred outside of the United States. The Massachusetts law does not contain any express provisions regarding

international data transfers. With respect to transfers to third parties in general, under the Massachusetts law, every information security program must include all reasonable steps to (i) verify that any third party service provider with access to personal information has the capacity to protect such information in the manner provided for in the Massachusetts Regulations and (ii) ensure that such third party service provider is applying security measures to personal information that are at least as stringent as those required under the Massachusetts Regulations.

ENFORCEMENT SANCTIONS

HIPAA: Penalties for non-compliance with HIPAA may include civil monetary penalties of between $100 to $50,000 per violation with a cap of $1,500,000 per calendar year. However, if a violation was not due to willful neglect and was corrected within thirty days after the entity knew or should have known about the violation, no penalty will apply. Alternatively, criminal penalties of a fine up to $50,000 and up to one year of imprisonment may apply. If the wrongful conduct involved false pretenses, the criminal penalties increase to a fine of up to $ 100,000 and up to five years of imprisonment. If the wrongful conduct involved the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm, the penalties increase further, to a fine of up to $250,000 and up to 10 years of imprisonment.

COPPA: Penalties for non-compliance with COPPA are provided for under the Federal Trade Commission Act, as a violation of COPPA is deemed to be an unfair or deceptive act. Penalties may include FTC enforcement actions and/or monetary penalties of $16,000 per violation.

FTC ACT: Penalties for violation of the FTC Act may include injunction and/or monetary penalties of up to $16,000 per violation.

STATE LAWS: Penalties for non-compliance with state breach notification laws and state information security laws vary by state. Generally, penalties for non-compliance with state breach notification laws range from injunctions, civil penalties from $100 to $750,000 per violation (larger for continuing violations), and private rights of action. The California breach notification law provides for injunctions and private rights of action. Penalties for non-compliance with state information security laws generally provide for civil penalties ranging from $1,000 per violation and up to $750,000 per violation for continuing violations. The Massachusetts information security law provides for civil penalties of up to $5,000 per violation and may require the violator to pay reasonable costs of investigation and litigation for the violation. Additionally, the Massachusetts State Attorney General may bring an action and Massachusetts state courts may issue injunctions.

EUROPE

EUROPEAN UNION

EUROPEAN UNION PRIVACY IN BRIEF

- Omnibus data protection law that covers all types of personal information, but generally no separate law regarding health privacy.
- Generally, health data is classified as "sensitive data", so processing health data is permissible only in limited circumstances.
- The transfer of data outside of the European Union may be prohibited unless the recipient country's laws provide "adequate protection" for the data or the recipient otherwise addresses this restriction.
- The European Union may soon implement a Data Protection Regulation, which would impose the same data protection and privacy requirements for the entire EU.

Introduction to Applicable Laws

Unlike the United States, Europe has an omnibus data protection law that covers all types of personal information, including health information. However, there is no separate law regarding health privacy specifically. This section summarizes the main aspects of the European omnibus law and of a representative group of member-state privacy legislation and how these laws may be applied to mHealth.

EU Data Protection Directive 95/46/EC

The European Union has adopted the EU Data Protection Directive 95/46/EC ("Data Protection Directive") in 1995. The Data Protection Directive sets the general principles and legal framework which had to be implemented into local law by the Member States. Hence, data privacy law is regulated ultimately at the national level.

Under the Data Protection Directive, and under the Member States law implementing the Data Protection Directive, health data relating to an individual person qualify as so-called sensitive data. According to the Data Protection Directive, the processing[45] of health data shall generally be prohibited, unless (i) the patient has given his explicit consent to the processing of his health data,

45 The term "processing" in this context encompasses the collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, erasure or destruction of personal data collection.

except where the local laws of the Member State exclude patient's consent for such purpose, (ii) processing is necessary for the purposes of carrying out the obligations and specific rights of the data controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards, (iii) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; (iv) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed to a third party without the consent of the data subjects, (v) the processing relates to health data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims, (vi) the processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided those health data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Proposed European Regulation on Data Protection

In January 2012, the European Commission released a draft European Data Protection Regulation which will at some point replace the Data Protection Directive. As opposed to an European directive, the proposed European regulation would apply immediately rather than needing to be implemented into local law by member states. The main objective of the European Data Protection Regulation is providing uniformity, the same level of data protection throughout the European Member States and thereby a higher level of legal certainty by preventing substantial deviations due to the local implementation process.

The draft European Data Protection Regulation is currently being debated by the European Union but is not expected to come into effect before 2016.

Germany — Federal Data Protection Act

Germany has implemented the Data Protection Directive with the German Federal Data Protection Act ("German Data Protection Act"). The German Data Protection Act defines health data as "sensitive data", which requires that organizations provide more comprehensive protection for health data. The processing of health data as sensitive data is generally only permissible if (i) the patient consented, (ii) the processing is necessary in order to protect vital interests of the patient or of a third party, in so far as the patient is unable to give his

consent for physical or legal reasons, (iii) the health data concerned has evidently been made public by the patient, (iv) the processing is necessary in order to assert, exercise or defend legal claims and there is no reason to assume that the patient has an overriding legitimate interest in excluding such processing, (v) the processing is necessary for the purpose of scientific research, where the scientific interest in carrying out the research project substantially outweighs the patient's interest in excluding the processing, and the purpose of the research cannot be achieved in any other way or would otherwise necessitate disproportionate effort, (vi) the processing is necessary for the purposes of preventive medicine, medical diagnosis, health care or treatment or the administration of health services and the processing of these health data is carried out by medical personnel or other persons who are subject to an obligation to maintain secrecy (Sec. 28 (6) of the German Data Protection Act).

UK Data Protection Act

UK has implemented the Data Protection Directive with the UK Data Protection Act 1998 ("UK Data Protection Act"). Sec.2 (e) of the UK Data Protection Act defines health data as "sensitive data", which requires that organizations provide more comprehensive protection for health data. The processing of health data as sensitive data is generally only permissible if (i) the patient has given his explicit consent to the processing, (ii) the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment, (iii) the processing is necessary in order to protect the vital interests of the patient or another person, in a case where (a) consent cannot be given by or on behalf of the patient, or (b) the data controller cannot reasonably be expected to obtain the consent of the patient, (iv) the processing is necessary in order to protect the vital interests of another person, in a case where consent by or on behalf of the patient has been unreasonably withheld, (v) the processing is carried out in the course of its legitimate activities by any body or association which is not established or conducted for profit, and exists for political, philosophical, religious or trade-union purposes, with appropriate safeguards for the rights and freedoms of data subjects, only relating to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, provided the processing does not involve disclosure of the health data to a third party without the consent of the patient, (vi) the information contained in the health data has been made public as a result of steps deliberately taken by the patient, (vii) the processing (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights, or (viii) the processing is necessary for medical

purposes, including the purposes of preventive medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services, and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

In addition to the UK Data Protection Act, the UK legislator has issued the Data Protection (Processing of Sensitive Personal Data) Order 2000 which sets out additional circumstances in which sensitive data may be processed. Such additional circumstances permit the processing of sensitive data for a range of other purposes, primarily purposes that are in the public interest and where patient's consent cannot be obtained.

Coverage by Data Protection Directive

PERSONS/ENTITIES OBLIGATED TO COMPLY

Any natural or legal person, public authority, agency or any other body which processes personal data, acting as a data controller or a data processor, must comply with the principles and requirements established by the Data Protection Directive and transported into local Member State law.

PERSONAL DATA

Personal Data is defined as any information relating to an identified or identifiable natural person. An identified person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Typically, any information that is associated with an individual's name, address, phone number, email address, or date of birth is considered personal data if it is theoretically possible to identify the individual.

SCOPE OF COVERAGE

The Data Protection Regulation applies to the collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, erasure or destruction of personal data (collectively "processing"), that is, basically anything one can do with data, provided the processing is carried out by automatic means (IT-system, computers, mobile devices, etc.) or by a non-automatic filing system (a structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographic basis).

INFORMATION REQUIREMENTS

According to the Data Protection Directive, the patient must generally be informed prior to the processing of his health data about (i) the identity of

the natural or legal person that processes the health data, (ii) the purposes of the processing for which the health data are intended, (iii) the recipients or categories of recipients to whom the health data is disclosed, (iv) whether the provision of personal data is obligatory or voluntary as well as the possible consequences if personal data is not provided, (v) the existence of the right to access to and the right to rectify the personal data.

CONSENT REQUIREMENTS

If the processing of health data cannot be justified by a statutory ground, (see above a. i. (ii) to (iv)) the Data Protection Directive requires that the patient's consent to the specific processing activities must be obtained. The Data Protection Directive defines consent as any freely given specific and informed indication of the data subject's wishes by which the data subject signifies his agreement to the processing of his personal data. Hence, in order to obtain valid consent, the patient must be informed comprehensively about the processing activities and be given the free choice whether or not he wants to consent.

DATA SECURITY OBLIGATIONS

RETENTION

Personal data, including health data, shall be kept in a form which permits identification of the patient for no longer than is necessary for the purpose for which the health data were collected or for which they are further processed. That is, once the purpose has been achieved, the health data must principally either be deleted or de-identified so that the health data cannot be associated with an individual.

SECURITY (INCLUDING CLOUD STORAGE)

According to the Data Protection Directive, the data controller must implement appropriate technical and organizational security measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of personal data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures must ensure a level of security appropriate to the risks represented by the processing and the nature of personal data to be protected. Typically, the level of security must be higher for health data as sensitive data.

If a data controller (e.g., a physician or a hospital) engages a third party service provider to store the health data on external services, the data controller must (i) diligently choose a third party service provider that provides sufficient guarantees in respect of the technical and organizational security measures and (ii) ensure compliance with those technical and organizational security

measures. This requirement of diligently choosing and continually monitoring a third party service provider also applies to any sub-processors a third-party service provider engages. With respect to cloud solutions where numerous service providers are engaged, the data controller is strictly speaking required to diligently choose every single one of them and to continually monitor all of them. Hence, in practice it will be very difficult, even impossible to comply with those requirements if personal data is stored in a cloud solution.

BREACH NOTIFICATION OBLIGATIONS

The Data Protection Directive does not impose any general security breach notification provision. However, the EU Directive on privacy and electronic communication 2002/58/EC ("ePrivacy Directive") provides that in case of a personal data breach, the provider of publicly available electronic communications services[46] must, without undue delay, notify the personal data breach to the competent supervisory authority. Furthermore, in case the personal data breach is likely to adversely affect the personal data or privacy of a subscriber[47], the provider of publicly available electronic communications services must also notify the subscriber of the breach without undue delay.

However, despite the lack of an overarching security breach notification requirement by the Data Protection Directive, several local Member States laws have imposed a notification obligation if certain categories of personal data are concerned. For example, the German Data Protection Act requires that a non-governmental body must notify both the patient and the responsible data protection authority without undue delay if it establishes that health data has been unlawfully transferred, or that unauthorized third parties have obtained the data, so that the patient's rights are at risk of harm.

DATA TRANSFERS (INCLUDING CROSS-BORDER)

Transfer of health data to another body (including an affiliate or a branch of the original data controller) will typically require the patient's consent unless the transfer is otherwise permitted by law. Furthermore, if the recipient is located in a country whose laws are not recognized as providing an adequate level of data protection[48], an adequate level of data protection must either otherwise be established or an exception to the requirement of an adequate

46 Electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.

47 Subscriber means any natural person or legal entity who or which is party to contract with the provider of publicly available electronic communications services for the supply of such services.

48 Countries recognized as providing an adequate level of data protection are in particular countries within the EU/EEA, Argentina, Israel, Switzerland, and Uruguay.

level of data protection must apply. An adequate level of data protection can be established above all by means of a Safe-Harbor certification of the recipient[49], the conclusion of so-called EU Model clauses, or within a group of company by means of binding corporate rules. An exception to the requirements of establishing an adequate level of data protection is given, amongst others, if (i) the patient consents to the transfer, (ii) the transfer is necessary for the performance of a contract between the patient and the data controller or the implementation of pre-contractual measures taken in response to the patient's request, (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and third party, (iv) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims, or (v) the transfer is necessary in order to protect the vital interest of the patient.

ENFORCEMENT AND SANCTIONS

The Data Protection Directive does not set out a catalog of sanctions in case of a breach. Instead, the Data Protection Directive instructs the Member States to adopt suitable measures to ensure the full implementation of and compliance with the Data Protection Directive. For example, under the German und the French Data Protection Act, administrative fines of up to EUR 300,000 per incident can be imposed. In certain circumstances, criminal sanctions, such as imprisonment may also be imposed.

ASIA-PACIFIC

AUSTRALIA

Introduction to Applicable Laws

Similar to Europe, Australia has an omnibus data protection law, also covering health information, but has not enacted a specific health privacy law. The National Privacy Principles ("Principles"), incorporated into the Privacy Act[50] set forth key principles regarding the handling of personal information by private sector legal entities. The Principles address data collection, use, disclosure, access and correction, cross border data transfers, and sensitive data, in addition to other issues.

49 Only available for bodies in the U.S.

50 The National Privacy Principles will be replaced with the updated Australian Privacy Principles ("APPs") under the recent amendments to the Privacy Act. These changes will go into effect in March 2014. The APPs are categorized into five groups of principles that are intended to cover the life cycle of handling personal data. In total, there are thirteen principles across the five groups.

AUSTRALIA PRIVACY IN BRIEF

- Similar to Europe, has an omnibus data protection law that covers all types of personal information, but generally no separate law regarding health privacy.
- Consent is relevant to many decisions about how health information is collected, used or disclosed.

Australia Privacy Act, 1988 ("Privacy Act")

Section 95 of the Privacy Act enacts a statutory body which has the authority to issue guidelines with respect to collection of information for public health and safety.

All organisations that provide a health service are covered by the Privacy Act (whether or not they are small businesses). Organisations providing a health service include:

- Traditional health service providers such as private hospitals and day surgeries, doctors, and specialists
- Pharmacists
- Allied health professionals such as psychologists
- Complementary therapists like naturopaths and chiropractors; and
- In some cases other services like gyms, fitness services and weight loss clinics, child care, and schools (if they provide a health service and hold health information).

Health information is personal information:

- Individual's health or disability at any time (that is, past, present or future)
- Individual's expressed wishes regarding future health services
- Health services provided, or to be provided, to the individual
- Collected whilst providing a health service; or
- Collected in connection with the donation or intended donation of body parts and substances.

Consent Requirements

Consent is relevant to many decisions about how health information is collected, used, or disclosed. Consent is not, however, required by the Privacy Act in all situations. The Privacy Act states that, in the context of the National Privacy Principles, consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent is an agreement that can be inferred from an individual's conduct.

The key elements to consent are:

- It must be provided voluntarily
- The individual must be adequately informed; and
- The individual must have the capacity to understand, provide and communicate their consent.

Data Security Obligations

RETENTION (INCLUDING CLOUD STORAGE)

Health information is highly valuable for many reasons, most importantly for an individual's on-going health care, but sometimes also for wider public health and safety reasons. Some State and Territory legislation, or guidelines issued by health professional organisations, require or recommend the retention of health information by health service providers for varying periods of time.

Under National Privacy Principle 3 health service providers must take reasonable steps to ensure that the personal information they collect, use, or disclose is accurate, complete, and up-to-date.

SECURITY

National Privacy Principle 4 requires that a health service provider take reasonable steps to:

- Protect the health information it holds from misuse and loss, as well as from unauthorised access, modification, or disclosure; and
- Destroy or permanently de-identify health information that is no longer needed.

IDENTITY AND AGE VERIFICATION PRACTICES

National Privacy Principle 8 sets out a health service provider's obligation to make available to individuals the option of not identifying themselves when entering transactions with the provider, wherever this is lawful and practicable.

BREACH NOTIFICATION OBLIGATIONS

Not applicable

Data Transfers (including cross-border)

Under National Privacy Principle 9, a health service provider may transfer personal information outside of Australia only under certain, specified circumstances. These circumstances include where the recipient is subject to local laws that provide protections for personal information that are substantially similar to the protections under the Privacy Act, the affected individual consents to the transfer or the health services provider has taken

reasonable steps to ensure that the recipient will not handle the data in any way that will violate the Principles.[51]

JAPAN

JAPAN PRIVACY IN BRIEF

- Japan employs a hybrid approach with industry-specific (or sectoral) privacy laws and a limited overarching privacy law.
- Japan's overarching privacy law applies to business operators that collect and store Personal Information on databases of more than 5,000 individuals.
- Generally requires the database operator to notify data subjects of the purpose of use of the Personal Information collected and obtain consent under certain limited circumstances.
- The law does not specifically address cross-border data transfers.

Applicable Law

The Act on the Protection of Personal Information (Act No. 57 of 2003) (the "Law") came into full effect on April 1, 2005. The Law establishes procedures for issuing rules for specific industrial sectors. Multiple government agencies that are responsible for the particular sectors have issued a number of guidelines pursuant to the Law's procedures.

Coverage

The Law applies to business operators that collect and store Personal Information on a database ("Data Controllers"). However, the Law does not apply to Data Controllers whose databases hold data about no more than 5,000 individuals on any given day in a six-month period.

The Law covers "Personal Information," which it defines as "[any] information that may make a living individual distinguishable from others." Personal Information would therefore cover a person's name, address, birth date, birth place, phone number as well as medical history. The Law distinguishes Personal Information from "Personal Data," which applies to information about the Data Controller's database.

51 Principle 8 of the new Australian Privacy Principles ("APPs") slightly modifies the conditions for cross-border transfer. Principle 8 first requires that the entity making the transfer take steps to ensure that the recipient of the data will not violate the APPs and then sets out exceptions to this requirement. The exceptions, similar to the conditions for disclosure under National Privacy Principle 9, include informed consent from the individual whose data is subject to the transfer that the transferring entity need not take steps to ensure that the recipient complies with the Principles.

Because the Law applies to medical history as covered Personal Information, the Law would generally apply to mobile health providers that store individual medical information on their databases, provided the health providers maintain records for over 5,000 individuals at one time.

Consent Requirements

Upon collecting Personal Information, the Data Controller must notify the data subjects of the purpose of use for the Personal Information collected. In general, a Data Controller must obtain express consent from data subjects if the Data Controller intends to use the Personal Information in any manner that is outside of the scope of the Data Controller's specified purpose or purposes of use.

Right to Access and Correct

In general, the Data Controller must disclose to data subjects, in writing or another means acceptable to the data subjects, the Personal Information processed upon their request.

If the Personal Information is found to be incorrect, the Data Controller must correct it within the scope of the specific purpose or purposes of use.

Data Security Obligations

The Law requires the adoption of technical, organizational and personnel security control measures to prevent leakage, loss or damage of Personal Information.

Data Transfers

The Law does not specifically address cross-border data transfers.

With respect to transfers to third-party processors, the Data Controller is required to exercise supervision over third-party processors to ensure the security of the Personal Information.

Enforcement and Sanctions

In the event of a data security breach, the relevant government agencies may collect reports from, advise, instruct and/or give orders to a Data Controller. If the Data Controller fails to comply with an administrative order, the Data Controller may be subject to penalties including imprisonment not exceeding six months or a monetary fine not exceeding ¥300,000. In addition, employees, agents or representatives of the Data Controller who violate the Law in the course of their duties and fail to comply with administrative orders may be subject to the same range of penalties. Where an employee, agent or representative of the Data Controller is subject to such penalties, the Data Controller may also be subject to a monetary fine not exceeding ¥300,000.

The Data Controller may also be required to pay compensation damages to affected data subjects as a result of tort or contract claims under the Japanese Civil Code. The Data Controller may also be required to compensate data subjects for reputational damages.

SINGAPORE

SINGAPORE PRIVACY IN BRIEF

Singapore's new law follows the European approach and constitutes an omnibus data protection law with cross-border transfer restrictions and specific notice and consent requirements.

Applicable Law

The Personal Data Protection Bill was passed in Parliament on 15 October 2012, and will be known as the Personal Data Protection Act ("PDPA") once it becomes an Act of Parliament. The PDPA came into force in January 2013.

The purpose of the PDPA is to regulate the collection, use and disclosure of personal data by organizations in a manner that recognizes both the right of individuals to protect their personal data, as well as the need of organizations to collect, use or disclose personal data.

The PDPA will be implemented in phases over 18 months, to allow organizations time to implement the necessary measures to comply with the PDPA.

Scope

The PDPA applies to all persons, companies and other organizations in Singapore, subject to certain exceptions in the public sector, such as the Government or any statutory body.

Personal data is widely defined in the PDPA. It refers to all data (in electronic or non-electronic form), from which an individual, living or deceased, can be identified, whether from that data or from other information which the organization has or is likely to have access.

The PDPA is intended to prescribe the baseline requirements for processing of personal data by organizations, and does not recognize a special category of personal data as sensitive personal data.

Consent Requirements

The PDPA requires that an individual's consent be obtained before an organization can collect, use, or disclose personal data unless required or authorized under the PDPA or any other written law. There are two forms

of consent – express and implicit. In the case of minors under the age of 18, consent can be given by an authorized representative (e.g., a parent or legal guardian, under a power of attorney, or any person with written authorization to act on an individual's behalf).

As a safeguard, an organization may collect, use, or disclose personal data about an individual only if the individual has been informed, and for the purposes that a reasonable person would consider appropriate in the circumstances.

The PDPA provides for some exceptions from obtaining consent, including but not limited to:

- Situations where the collection of personal data is necessary to respond to an emergency that threatens the life, health, or safety of the individual or another individual
- By employers for purposes of managing or terminating an employment relationship
- Disclosure to a public sector or law enforcement agency
- Disclosure pursuant to a subpoena, warrant, or court order
- Disclosure of personal data of an organization's employees, customers, or shareholders to a prospective purchaser in a merger or acquisition transaction, provided that such information should be destroyed or returned if the transaction falls through.

An individual, upon giving reasonable notice to the organization, may withdraw the consent. Once withdrawn, the organization shall cease collecting, using, or disclosing the personal data.

Right to Access and Correct

Individuals have rights under the PDPA to:

- Request information about their personal data that is in the possession or control of an organization
- Obtain information about the ways which their personal data has been or may have been used or disclosed by the organization
- Request an organization to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organization.

The organization is obliged under the PDPA to:

- Respond to the individual as soon as reasonably possible, assist the individual to obtain access to the personal data collected, and provide the individual with information about the ways in which such personal data has been used and to whom the personal data has been disclosed, subject to various exceptions

- Correct the personal data as soon as possible and send the corrected personal data to every other organization to which the personal data was disclosed by the organization within a year before the correction was made, unless there are reasonable grounds that a correction should not be made.

Data Security Obligations

Obligations imposed on the organization under the PDPA to ensure that the personal data is properly cared for:

- ACCURACY OF PERSONAL DATA Organizations must make a reasonable effort to ensure that the personal data collected is accurate and complete, if the personal data is, among other things, likely to be used by the organization to make a decision that affects the individual to whom the personal data relates
- PROTECTION OF PERSONAL DATA Organizations must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorized access, collect, use or similar risks
- RETENTION OF PERSONAL DATA Organizations must delete or anonymise documents containing personal data as soon as it is reasonable to assume that the purpose of collecting the data is no longer served by its retention, and retention is no longer necessary for legal or business purposes.

An organization is required to protect personal data in its custody or under its control by putting in place reasonable security measures to prevent unauthorized access to or use of such data. However, the PDPA does not prescribe any specific methods of securing personal data or specific standards that organizations need to adhere to.

Breach notification requirements are not covered in the PDPA. However, specific requirements for particular industries may be imposed by sectoral laws, codes of practice, or guidelines.

Data Transfer (including cross-border)

The PDPA adopts a "principle-based approach" and provides that organizations transferring personal data outside of Singapore are required to ensure that appropriate measures are put in place to safeguard the personal data.

In general, organizations are not allowed to transfer any personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA. This is to ensure that personal data is accorded a similar level of protection under the PDPA even if it was transferred outside Singapore.

Enforcement and Sanctions

A Personal Data Protection Commission will be set up to undertake education and awareness efforts and oversee the implementation of the PDPA. Powers of the commission include:

- Review of complaints
- Giving directions to remedy non-compliance
- Imposing a financial penalty of up to S$1 million
- Imposing criminal penalties on organizations or individuals who obstruct the Commission in the performance of its duties or functions, or knowingly or recklessly make false statements to mislead the Commission, or for failure to comply with an order issued by the Commission.

In order to keep compliance costs down for organizations, the Commission will adopt a complaint-based approach in exercising its oversight duties, and will only investigation cases of non-compliance where a complaint is filed. Organizations will not be required to submit reports to, or be audited by, the Commission on a regular basis.

The PDPA also enables individuals to seek redress against an organization for breach of the PDPA via civil proceedings.

LATIN AMERICA

ARGENTINA

ARGENTINA PRIVACY IN BRIEF

- Argentina also has an omnibus data protection statute and follows the European approach.
- Express consent from the data owner is generally required when collecting "sensitive data", including health data but there are exceptions for some health care professionals.
- Data owners have the right to request and obtain information on their personal data that is included in a data bank.

Applicable Law

Personal data protection is regulated by the Personal Data Protection Law ("PDPL") No. 23.326, which became effective on 10 November 2000, and was restated by Regulatory Decree No. 1558/2001 ("Decree").

The Argentine Constitution ("Constitution") also provides for a special judicial remedy known as "habeas data" to protect personal data, thereby upgrading the protection of personal data to the category of fundamental rights.

The PDPL, together with the Decree, the Constitution and certain resolutions issued from time to time by the Argentine Protection Authority, govern the protection of personal data in Argentina.

Scope

The PDPL applies to anyone owning a database, including individuals or legal entities, either public or private.

The PDPL defines personal data as information of any kind referring to ascertainable physical persons or legal entities. Argentine law protects personal data used for reporting purposes and recorded in data files, registers, databases, or by other technical means.

The PDPL also recognizes a special category of personal data as sensitive data, namely any personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior.

The PDPL provides that data owners cannot be compelled to provide sensitive personal data, except in health-related and union membership cases or where such information is necessary for employment purposes. It is prohibited to create files, banks, or registers storing information that directly or indirectly reveal sensitive personal data.

Consent Requirements

Under the PDPL, the treatment of personal data is unlawful when the data owner has not given his or her express consent in writing, or through any similar means, depending on the circumstances. The consent must appear in a prominent and express manner. Consent must be an informed consent, and is revocable by the data owner.

There are however some exceptions set out in Section 5, Paragraph 2 of the PDPL. Consent shall not be deemed necessary when personal data:

- Is secured from a source of unrestricted public access
- Is collected for the performance of the duties inherent in the powers of the State
- Consists of lists limited to name, national identity card number, taxing or social security identification, occupation, date of birth, domicile, and telephone number
- Is necessary for the development or compliance of a contractual, scientific, or professional relationship with the data owner.

The PDPL requires express consent from data owners for the processing of sensitive personal data. Exceptions to this rule are:

- Processing of sensitive personal data for reasons of general interest authorized by applicable laws
- Processing of sensitive personal data for statistical or scientific purposes, provided that data owners cannot be identified
- Processing of sensitive personal data referring to records on criminal or other offences, provided that the same is processed only by competent public authorities within the framework established by applicable laws and regulations
- Processing of sensitive personal data relating to the physical or mental conditions of patients by public or private health institutions, and medical science professionals, in pursuance of the principles of professional secrecy.

There is no provision in the PDPL that specifically addresses consent requirements for minors.

Whenever personal data is requested, data owners must be previously notified in an express and clear manner:

- The purpose for which the data shall be treated and to whom the data will be addressed
- The existence of the relevant data file, register, or bank, whether electronic or otherwise, and the identity and domicile of the person responsible
- The compulsory or discretionary character of the answers to the questionnaire the data owner is presented with, in connection with sensitive personal data
- The consequences of providing the data, or of refusing to provide such data or of providing inaccurate data
- The avenues available to the data owner to exercise his or her right of data access, rectification, or suppression.

Disclosures of Personal Data

Personal data may be disclosed only to meet the purposes directly related to the legitimate interests of the person responsible for the data file and the recipient and with the data owner's consent. The data owner must be informed about the purpose of such communication and the identity of the intended recipient. Consent of the data owner for such disclosure is revocable.

Consent is not required when:

- A law so provides
- There exists circumstances set forth in Section 5, Paragraph 2 of the PDPL
- Communication of the data takes place directly between government agencies, to the extent of their corresponding competencies

- The data communicated is health-related personal data, and it is necessary to communicate such data for public health or emergency reasons, or for conducting epidemiological surveys, provided the identity of the data owner is kept confidential.

Right to Access and Correct

Data owners have the right to request and obtain information on their personal data included in public or private data registers or banks with reporting functionality. They must be provided the requested information within 10 calendar days of making such request, or the data owner may commence habeas data proceedings to protect his/her personal data.

All persons have a right to rectify, update and when applicable, suppress or keep confidential their personal data included in a data bank, except that such suppression must not be effected if it could cause harm to the rights or legitimate interests of third parties, or a legal obligation exists to preserve such data.

The person responsible for or the user of the data bank must proceed to rectify, update or suppress the personal data belonging to the data owner by performing the operations necessary for such purpose within five business days of receipt of the complaint or notice of the mistake or false information.

Non-compliance with this obligation within the time stipulated above will enable all data owners to commence habeas data proceedings to protect their personal data.

The person responsible for or the user of the data bank must notify recipients of the rectified or suppressed data within five business days of the rectification or suppression.

The persons responsible for or users of public data banks may deny the access to or the rectification or suppression of personal data in the following cases:

- Based on national defence, public order and safety grounds
- For the protection of rights and interests of third parties
- When such data could hinder pending judicial or administrative proceedings relating to the compliance with tax or social security obligations, the performance of health and environment control functions, the investigation of crimes, and the verification of administrative violations.

Data Security Obligations

The person responsible for or the user of data files must take such technical and organizational measures as are necessary to guarantee the security and confidentiality of personal data, in order to avoid their alteration, loss, unauthorized consultation or treatment. These measures should also allow for the detection of any intentional or unintentional distortion of such information.

Under Section 9 of the PDPL, it is prohibited to record personal data in files, registers or banks that do not meet the requirements of technical integrity and security.

There is no specific mandatory obligation under the current law to notify the authorities of a security breach. Practically, in the event of a security breach, the Argentine Protection Authority ("Authority") usually initiates an investigation to confirm whether the company affected by the security breach has adopted the security measures required by the PDPL and other regulations enacted by the Authority.

There is also no obligation under the PDPL to notify consumers about a security breach. However, companies affected by a security breach usually consider reporting the incident to their customers to allow them to adopt the appropriate course of action to protect their information and minimize damages.

Where the data security breach affects information that has been registered with the Authority (e.g., a database), such an incident must be reported to the Authority. The Authority generally requests the company to clearly explain the details of the security methods that are implemented to prevent third parties from using private information, and may punish the company if it concludes that the company has not implemented appropriate technical and organizational security methods.

Data Transfer (including cross-border)

The transfer of personal data to countries which do not provide adequate levels of protection is prohibited.

Prohibition shall not apply in the following circumstances:

- International judicial co-operation
- Exchange of medical information, when so required for the treatment of the data owner
- Exchange of medical information in case of an epidemiological survey, provided that the identity of the data owner is kept confidential
- Stock exchange or banking transfers in pursuance of applicable laws
- When the transfer is agreed upon within the framework of international treaties signed by Argentina.

When the transfer is made for international co-operation purposes between intelligence agencies in the fight against organized crime, terrorism, and drug-trafficking.

Enforcement and Sanctions

The Authority may impose the following administrative sanctions for non-compliance:

- Warnings

- Suspensions
- Fines ranging between 1,000 pesos and 100,000 pesos
- Closure or cancellation of the file, register, or database

The Authority actively conducts audits to confirm if processors of personal data comply with security obligations.

The following criminal penalties may also be imposed under the Argentine Criminal Code:

- Imprisonment for a term of one month to two years for anyone who knowingly inserts or has false information inserted in a personal data file
- Imprisonment for a term of six months to three years for anyone who knowingly provides a third party with false information contained in a personal data file
- Imprisonment for a term of six months to three years for anyone who:
  - Knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into a personal data bank
  - Discloses to third parties information registered in a personal data bank which should be kept secret by provision of law.

MEXICO

MEXICO PRIVACY IN BRIEF

Mexico's relatively new law (effective since 2010) follows the European omnibus approach.

Applicable Law

Federal Law for the Protection of Personal Data Held by Private Individuals (Ley Federal de Proteccion De Datos Personales en Posesion de los Particulares ("LFPDP" or "the Act"), effective July 6, 2010. The Ministry of Economics is responsible for disseminating information on obligations related to the protection of personal data to domestic private enterprise and international enterprise with business activity in Mexico.

Scope

The act applies to the processing of personal data by companies and persons on Mexican territory regardless of where the data subjects reside. As a consequence, Mexican-based Internet companies have to comply with the Mexican law regarding any personal data they collect on non-Mexican users. Also, a Mexican parent company would have to comply with the law with respect to data collected from employees of its foreign subsidiaries; however, the statute does not expressly extend to the processing of personal data relating to

Mexican residents by companies acting outside of Mexico. Therefore, it is likely that a U.S.-based Internet company would not be required to comply with the Mexican law as to data submitted by Mexican Internet users.

General Principles

The Mexican law follows the Organisation for Economic Co-operation and Development ("OECD") Guidelines and addresses the following principles:

Notice – The privacy notice plays an important role because it can be used to solicit tacit consent. Data subjects should be given notice when their personal data is being collected, including the following elements: (i) the identity and address of the data collector; (ii) the purposes for the collection of personal data; (iii) the options and means implemented by the data collector to limit the disclosure or use of the data; (iv) the mechanisms that the data subjects can follow to request access, correction, cancellation and opposition as provided by the data protection law; and (v) the process through which the data collector will communicate to the data subjects the changes in the privacy notice.

- Purpose – Personal data should only be used for the stated purposes and not for any other purposes
- Consent – Personal data should not be disclosed without the data subject's consent
- Security – Personal data should be kept safeguarded from potential abuses
- Disclosure – Data subjects should be informed about the identity of the data collector
- Access – Data subjects should be allowed to access their data and make corrections to any inaccurate data
- Accountability – Data subjects should have a method available to them to hold data collectors accountable for breaches of the above principles.

Coverage

The Act covers processing of personal data by individual persons or private legal entities, with the exception of credit reporting companies and private individuals collecting and storing exclusively for personal use without purposes of disclosure or commercial use.

As under European Union law, the terms "processing" and "personal data" are defined broadly and cover "the procurement, use (including any access, management, transfer or disposal), disclosure or storage of personal data by any means " of any" information concerning an identified or identifiable individual." Mexico also follows the European approach to generally prohibit the processing of personal data, as a default, by requiring that one of the following conditions is met: (i) consent; (ii) a necessity under contract or statute; or (iii) superseding interests based on a balancing test of interest and emergency situations. With

respect to data available from public sources, Mexico is more lenient than Europe and generally permits processing of such data without consent or other justification.

Interestingly, the new Mexican law refers to data subjects as "titulares;" (i.e., the "owner") but the statute itself does not create property rights in personal data for data subjects, except if the data consists of a photograph of the subject.

Consent Requirements

Where consent of the data subject is required, consent may be given verbally, in writing, by electronic or optical means or any other technology or by unmistakable means. If the data subject receives a privacy notice and does not object to the terms of the notice, it is understood that the data subject has given tacit consent.

Consent may be revoked at any time, but the revocation cannot be applied retroactively. The data controller must set out revocation mechanisms and procedures in the privacy notice.

Express consent is required before an organization may process sensitive personal data. "Sensitive personal data" is defined as "Personal data touching on the most private areas of the data owner's life, or whose misuse might lead to discrimination or involve a serious risk for said data owner. In particular, sensitive data is considered that which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views, sexual preference". The privacy notice must expressly state that the organization collects and processes sensitive data.

Although generally data owners have the right to cancel their own data, the data controller is not obligated to cancel personal data when it is subject to processing for medical diagnosis or prevention or health services management, provided such processing is done by a health professional subject to a duty of secrecy.

Data Security Obligations

The Mexican law provides for much broader notification obligations than U.S. state laws and the laws currently considered or recently enacted in Europe. Breaches to the security of personal data that affect the patrimonial or moral rights of data subjects in a material manner must be immediately communicated to the data subjects.

Additionally, personal data must be deleted if it is no longer required for the purposes indicated in the privacy notice provided to the data subjects.

Similar to European law and the general trend of evolving data security standards, all data processors must implement and maintain the administrative, technical, and physical measures that protect personal data from damage, loss, alteration, destruction or unauthorized use, access, or treatment. Security measures implemented must not be less than those used by data collectors to protect their own information and must also take into account the existing risk and the consequences derived from the sensitivity of the data and the prevalent technical development.

Data Protection Authorities / Data Protection Officers

Companies do not have to register databases or notify their data processing activities to any government authority.

All data controllers and processors have to appoint a person or group as being responsible for personal data-related requirements; e.g., a company privacy officer. Employers have to appoint a person or establish a personal data department in charge of handling employees' personal data and promoting the protection of the same.

Data Transfer (including cross-border)

Companies may not transfer personal data within Mexico or abroad unless they notify such transfers in the applicable privacy notice to the data subjects. If so notified, transfers are permitted without consent of the data subjects in certain exceptional circumstances including, for example, when the transfer is made between companies of the same controlling group; otherwise, consent is required. Unlike under EU law, international transfers are not specifically restricted, and Mexican companies do not have to obtain government authorization or ensure "adequate safeguards" of data recipients outside Mexico.

Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data. The third party receiver will assume the same obligations as the data controller that has transferred the data.

ARTICLE 37: Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases:

4.a Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management.

4.b Where the transfer is necessary by virtue of a contract executed or to be executed in the interests of the data owner between the data controller and a third party.

Enforcement and Sanctions

Article 63 sets out nineteen separate examples of actions and inactions that are violations of the legislation. These actions include failure to respond to the data owner's request to access, rectify, cancel, or object to the personal data held or the data controller acting negligently or fraudulently in processing and responding to requests for personal data access.

Violations are punishable by fines based on a multiple of Mexico City's minimum wage and will vary depending on the seriousness of the violation. Fines range from 100 days to 320, 000 days of minimum wage. Those fines can be doubled for breaches involving sensitive personal data.

There are criminal sanctions including terms of imprisonment from 3 months to three years for any person who is authorized to process personal data for profit and causes a security breach affecting the databases under his custody.

Article 68 imposes a term of imprisonment from 6 months to five years for any person who, with the aim of achieving unlawful profit, processes personal data deceitfully, taking advantage of an error of the data owner or the person authorized to transmit such data.

As with the provisions for imposing fines, custodial sentences are doubled for breaches of sensitive personal data.

Data subjects have the right to enforce the protection of their personal data by complaining to the Mexican Institute for Access to Information and Personal Data ("IFAI") when a data collector refuses to take certain actions that are required by law. Upon notice of a resolution from the IFAI, data collectors have 10 days to comply with the resolution. The IFAI may initiate an action to verify compliance with the data protection law by any data collector upon petition by an interested party or ex-officio. The IFAI may also initiate at any time a conciliatory process between a data subject and a data collector. Data subjects may further seek damages from data collectors when they consider that they have suffered harm or losses derived from a breach by the data collector of the new Mexican data protection law.

Compromising the security of a database containing personal data with the intention to profit is a criminal offense, which can be punished with up to three years of imprisonment and up to six years when sensitive personal data is involved.

Furthermore, the act of collecting, using, disclosing or storing personal data through deceit and with the intention to profit is also considered a criminal offense punishable with up to five years of imprisonment, and up to 10 years when sensitive personal data is involved.

AFRICA

Compared to other regions, particularly Europe and certain sectors of Latin America and Asia that have implemented omnibus privacy regimes and other privacy laws, privacy law in Africa is relatively undeveloped. Most African countries have not implemented comprehensive data privacy laws like those of Europe, and these countries have also not addressed privacy via a sector specific approach like that taken by the United States. Note that some countries, such as Mauritius, Morocco and Tunisia, have enacted comprehensive data protection laws, and others such as South Africa (whose legislation is anticipated to become law later in 2013) and Kenya have developed draft bills that have not yet come into force and/or been finalized. Implementation of omnibus privacy laws is not, however, the norm among African nations.

Many African nations also have not enacted laws that provide broad protection to health and medical data such as that provided by HIPAA in the United States. That is not to say, however, that there is a complete void of privacy protections in Africa, particularly with regard to health and medical data. Certain countries have constitutional protections for privacy, and health-related laws tend to focus on protecting the confidentiality of certain types of information, particularly health and medical data, data more specifically related to HIV/AIDS or other sub-categories of health and medical data, such as DNA or genetic information. Many of these laws impose their obligations on health and medical workers and other individuals who would normally have access to such categories of data and, in some countries, are supplemented with ethical codes of practice or similar rules for practitioners. The penalties for violations of such laws and codes vary widely.

MEDICAL ETHICS

As we discussed in the introduction, confidentiality is an aspect of patient privacy. It is a promise by the healthcare provider and recipient of mHealth data that the information will be kept in strict confidence and used only for the purposes for which it was entrusted. Medical ethics codes have long recognized the physician's obligation to safeguard a patient's medical information and these codes have evolved with the profession. In some countries, these codes are exclusively regulated by the profession itself, while, in others, the code is part of the national law. In still other jurisdictions, these obligations form part of everyday practice but are not codified in a formal way. Within these examples, there a variety of approaches. While it is true that medical ethics do not traditionally apply beyond the healthcare provider and patient relationship (excluding, for purposes of mHealth, all the other actors identified in Figure 4 above), they still merit review

here. The long-established role of medical ethics and patient confidentiality can provide helpful guidance and context to the discussion of mHealth privacy law issues, particularly in terms of weighing competing interests. Also, strong and well-established ethical codes can serve to strengthen and buttress any efforts at mHealth privacy legislation. Likewise, entrenched views on patient privacy rooted in ethical codes may pose a serious obstacle to adoption of mHealth laws and regulations that run counter to these conceptions.

THE SOURCES OF MEDICAL ETHICS

The Hippocratic Oath provides, "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account must be spread abroad, I will keep to myself, holding such things shameful to be spoken about." *"I Swear by Apollo Physician..."*[52] More recent articulations of the important healthcare ethical considerations involving privacy of medical information include that of Tom Beauchamp and James Childress, whose four principles (respect for autonomy, nonmaleficence, beneficence, and justice) inform a broad definition of "privacy."[53] The authors consider various types of privacy, advocating that "those who propose policies carefully specify the conditions of access that will and will not count as a loss of privacy or a violation of the right to privacy" and "define the zones that are considered private .... and ... identify interests that legitimately may be balanced against privacy interests."[54]

To define such interests (and propose how to balance them) is to assume that privacy rights are not absolute and that they may give way under certain conditions – a belief that is not universally held. And even where privacy rights are not absolute, identifying conflicting interests does not provide a basis for determining when privacy rights must yield, as determinations of this kind are likely to be made based more on degrees of risks and harms to others than on the mere fact that the interest is involved. Furthermore, interests identified as sufficient to overcome privacy rights in one community may be inadequate in another. This is so, in part, because concepts of "autonomy" and "privacy" that might inform the ethical principles of a community may be based on sources unique to it – for instance, oral traditions and religious beliefs, practices, and texts, legal history and codified law, medical or health issues specific to the region, and other practical considerations or limitations.

52 *Greek Medicine from the Gods to Galen*, as translated by M. North, National Library of Medicine, available at **http://www.nlm.nih.gov/hmd/greek/greek_oath.html**.

53 Tom L. Beauchamp & James Childress, Principles of Biomedical Ethics, 5th ed. (2001), at 295.

54 *Id.*

Nevertheless, to greater or lesser degrees, common principles of health privacy are reflected in many jurisdictions' medical ethics, be those codes discerned through practice, codified in law or written codes, or both. The following sections provide a brief overview of the disparate medical privacy ethics of various nations, illustrating both the difficulty of arriving at a common set of health-privacy norms and the importance of understanding the role of cultural values in the development and implementation of health privacy policies.

A comprehensive overview of world medical ethics[55] is beyond the scope of this section, but a brief consideration of health privacy ethics is informative for discerning the major principles and recognizing the differences that may exist among jurisdictions. The country-by-country illustrations presented here are not meant to imply that every nation adopts a single set of principles, as communities within nations may differ in their perceptions of health privacy and interest that may conflict with privacy rights. But a look at several nations' principles of health privacy, limited as they are in drawing generalities, serves to illustrate both the common principles that have emerged and the diversity in approaches worldwide. Additional information on health-privacy ethics is provided in the next section, "Case Studies".

THE UNITED STATES, CANADA, AND EUROPE

UNITED STATES

The American Medical Association Principles of Medical Ethics (2001) provides, "A physician shall respect the rights of patients, colleagues, and other health professionals, and shall safeguard patient confidences and privacy within the constraints of the law."[56] The obligation of confidentiality in the United States is a longstanding one; for instance, the 1847 version of the Principles adopted by the AMA recognized that the law protected physicians against the obligation of disclosure:

> Secrecy and delicacy, when required by peculiar circumstances, should be strictly observed ... The obligation of secrecy extends beyond the period of professional services; — none of the privacies of personal and domestic life, no infirmity of disposition or flaw of character observed during professional attendance, should ever be divulged by him except when he is imperatively required to do so. The force and necessity of this obligation are indeed so great, that professional men have, under certain circumstances, been protected in their observance of secrecy, by courts of justice.

55 See, e.g., Robert B. Baker & Laurence B. McCullough, *Cambridge World History of Medical Ethics*, vols. 1, 2 (2009).

56 See AMA Medical Ethics Principles, available at **http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/principles-medical-ethics.page**.

American Medical Association, Code of Medical Ethics of the American Medical Association, May 1847, ch. 1, art. 1.[57]

Today, likewise, health privacy ethics in the United States may be seen to be reflected in the law, as highlighted by the enactment of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy and Security Rules (which protect the privacy of individually identifiable health information and set national standards for the security of electronic protected health information) and the Patient Safety and Quality Improvement Act of 2005 ("PSQIA") Patient Safety Rule (which protects identifiable information being used to analyze patient safety events and improve patient safety). These statutes and Rules may be said to reflect the principle that health professionals have an affirmative ethical obligation to protect patient health privacy and that the national government has an oversight obligation to ensure that these privacy obligations are met. Additionally, state governments may regulate health information even more strictly than does the federal government; for instance, several U.S. states have enacted statutes specific to HIV status and medical records, prohibiting HIV information from being disclosed even where a general release of medical information has been obtained (and requiring a specific release for disclosure of the information).

Nevertheless, a patient's privacy right is not absolute. To take once again the example of HIV status and medical information, U.S. healthcare workers are obligated to report HIV infections and AIDS cases to public health authorities, including, recently, the patient's name and other identifying information. In addition, healthcare providers may, if they choose, disclose a patient's HIV infection to a sexual or needle-sharing partner of the patient. The Centers for Disease Control and Prevention ("CDC") has made specific recommendations for keeping reporting confidential and has recommended that anonymous testing for HIV continue to be made available. And again, some states, including California, have enacted laws requiring the patient's informed consent before a healthcare provider warns a patient's partner.[58]

CANADA

The Canadian Medical Association Code of Ethics (1996), like the American Medical Association Code, requires physicians to "respect the patient's right to confidentiality except when this right conflicts with [the physician's] responsibility to the law, or when the maintenance of confidentiality would result

57 Note that such protections against disclosure in the laws and rules that regulate court proceedings are essential to ensuring that privacy promises can be kept by those who make them. If the courts do not recognize the confidentiality of certain types of mHealth data, this creates a significant vulnerability in the privacy ecosystem and undermines it as a whole.

58 California Health and Safety Code §§ 120975-121020.

in a significant risk of substantial harm to others or to the patient if the patient is incompetent; in such cases, [the physician must] take all reasonable steps to inform the patient that confidentiality will be breached."[59] The Code also requires physicians to "[d]isclose patients' personal health information to third parties only with their consent, or as provided for by law."[60]

The Personal Information Protection and Electronic Documents Act ("PIPEDA") is a Canadian statute that codifies privacy protections based on the 10 privacy-related principles forming the Canadian Standards Association's Model Code for the Protection of Personal Information, which limits the collection and uses of health or other personal information.

As in the United States, Canadian medical ethics and law recognize exceptions to the rule of health information confidentiality. HIV and AIDS cases must be reported to provincial health authorities. Canadian law also recognizes a "public safety" exception to the rule of confidentiality. Although physicians in Canada are not obligated to breach patient confidentiality to protect others, the law is apparently unfixed in this regard, and physicians may disclose HIV status to sexual or injection partners of an infected patient.[61]

EUROPE

A country-by-country survey of the European Union[62] and other European nations is beyond the scope of this section. As such, it aims only to provide a sampling of various jurisdictions' position on medical ethics as related to privacy.

The European Convention on Human Rights protects the right to respect for private and family life, and also protects confidential information.[63] Ethical principles of privacy of medical and other personal information may be reflected in the European Commission's Data Protection Directive, 95/46/EC, which regulates and limits the processing and disclosure of personal information within the European Union. Still, efforts have been made to recognize universal principles of health privacy ethics. The World Health Organization's 1994 Declaration on the Promotion of Patients' Rights in Europe provides for

59 Canadian Medical Association Code of Ethics, available at **http://www.cma.ca/privacy-confidentiality**.

60 *Id.*

61 Dave Unger, *The Canadian Bioethics Companion: An Online Textbook for Canadian Ethicists and Health Care Workers* (2011), ch. 2, available at **http://canadianbioethicscompanion.ca/the-canadian-bioethics-companion/chapter-2-the-doctor-patient-relationship/**.

62 Ethical and legal code provisions of the EU Member States are available in *European Patients' Forum, Patients' Rights in the European Union*, available at **www.eu-patient.eu/Documents/Projects/Valueplus/Patients_Rights.pdf**.

63 See European Convention on Human Rights, Art. 8 ("There shall be no interference by a public authority with the exercise of th[e] right [to privacy] except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.").

autonomy ("Everyone has the right to self-determination") as well as privacy ("Everyone has the right to respect for his or her privacy.").[64] The Declaration, whose adoption is voluntary for Member States, sets forth several principles that reflect various nations' medical and ethical codes involving health privacy:

4.1 All information about a patient's health status, medical condition, diagnosis, prognosis and treatment and all other information of a personal kind must be kept confidential, even after death.

4.2 Confidential information can only be disclosed if the patient gives explicit consent or if the law expressly provides for this. Consent may be presumed where disclosure is to other health care providers involved in that patient's treatment.

4.3 All identifiable patient data must be protected. The protection of the data must be appropriate to the manner of their storage. Human substances from which identifiable data can be derived must be likewise protected.

4.4 Patients have the right of access to their medical files and technical records and to any other files and records pertaining to their diagnosis, treatment and care and to receive a copy of their own files and records or parts thereof. Such access excludes data concerning third parties.

4.5 Patients have the right to require the correction, completion, deletion, clarification and/or updating of personal and medical data concerning them which are inaccurate, incomplete, ambiguous or outdated, or which are not relevant to the purposes of diagnosis, treatment and care.

4.6 There can be no intrusion into a patient's private and family life unless and only if, in addition to the patient consenting to it, it can be justified as necessary to the patient's diagnosis, treatment and care.

4.7 Medical interventions may only be carried out when there is proper respect shown for the privacy of the individual. This means that a given intervention may be carried out only in the presence of those persons who are necessary for the intervention unless the patient consents or requests otherwise.

4.8 Patients admitted to health care establishments have the right to expect physical facilities which ensure privacy, particularly when

64 World Health Organization, Declaration on the Promotion of Patients' Rights in Europe (June 28, 1994), available at **www.who.int/genomics/public/eu_declaration1994.pdf**, at Arts. 1.2, 1.4.

> health care providers are offering them personal care or carrying out examinations and treatment.[65]

Many of these principles are reflected in the codified law in Member States. In the United Kingdom, General Medical Council ("GMC") guidance provides that patients have a right to expect that their physicians will keep their medical information confidential.[66] As in the United States and Canada, the obligation to protect confidential patient information is not absolute, and regulations recognize a reporting duty with respect to certain diseases. Also, as in the North American countries, a UK physician may alert a partner of an HIV-infected patient, regardless of whether the patient has given informed consent to the disclosure.[67]

In France, Article 4 of the Code of Medical Ethics promulgated by the Conseil National de l'Ordre des Médecins provides that professional confidentiality, instituted in patients' interest, is obligatory for every physician within the conditions established by law.[68] French Penal Code (Nouveau Code Pénal) Article 226-13 provides that the disclosure of confidential information acquired in any manner in one's professional capacity or by reason of a function or of a temporary mission is punishable by one year's imprisonment and a fine of 15,000 euros.[69] More specifically, a patient's HIV status is strictly protected under the Ordre des Médecins, which forbids physicians from making disclosures to partners of HIV-infected individuals who oppose the disclosure.[70] Data from a recent survey study supported the finding that most French physicians believe that breaching patient confidentiality is never acceptable, a view that is consistent with the official position of the Ordre des Médecins.[71]

LATIN AMERICA

BRAZIL

Healthcare workers in Brazil follow a strict code of medical ethics that precludes disclosure of patient information to any third party except where required by

65 *Id.* at Art. 4.

66 General Medical Council, *Confidentiality: Guidelines for Doctors* (Oct. 2009), available at . **http://www.gmc.org**.

67 Mike Williams, *Confidentiality of the Medical Records of HIV-Positive Patients in the United Kingdom – A Medicolegal and Ethical Perspective*, Risk Mgmt. Healthcare Policy, 4:15 (2011), available at **http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3270929/#b64-rmhp-4-015**.

68 C. Olivari, Maria Teresa Muñoz Sastre, Myriam Guedj, et al. *Breaking Patient Confidentiality: Comparing Chilean and French Viewpoints Regarding the Conditions of Its Acceptability, Universitas Psychologica*, 10(1):13, 14 (2011).

69 Again, statutory provisions such as these provide "teeth" to the privacy and confidentiality laws and ensure that they will not be trumped by other interests without a careful analysis of the issues at stake. Privacy law is unlikely to succeed in a vacuum without the support of other areas of the legal system.

70 *Id.*

71 *Id.* at 23.

law.[72] Health privacy is protected by professional confidentiality obligations; health professionals take an oath to protect patient privacy upon graduating to practice.[73] Medical confidentiality has historic origins and is ethically expressed in the Hippocratic Oath; the Medical Code of Ethics identifies standards governing professional conduct, including prohibitions and obligations related to privacy, as well as prerogatives of disclosure.[74] A healthcare professional's disclosure of patient information renders the professional subject to disciplinary action as well as criminal sanctions for harm caused to the patient, although such sanctions are rare and the bar against disclosure is not absolute where certain conflicts of interest arise.[75] Moreover, the physician is in control of the disclosure where the patient has consented to same: "After [patient] consent, the revelation becomes only optional, never obligatory, the final decision being the doctor's. It can be said that the consent for revelation results in the option of volitive deliberation."[76] A fundamental consideration as to whether to breach privacy is the harm to third parties.[77]

The right to privacy is not absolute; exceptions exist at law. For instance, the Brazilian Health Ministry has recently indicated that it will require physicians to report all new cases of HIV infection; previously, the reporting requirement was restricted to patients diagnosed with AIDS.[78]

ARGENTINA

In 2001, the Argentine Medical Association (*Asociación Médica Argentina*), the primary professional association of physicians in Argentina, published a Code of Ethics for the Health Team (*Código de Ética para el Equipo de Salud*); a second edition was pubished in 2011.[79] Chapter 7 of the Code sets forth the obligations of professional confidentiality as an ethical duty of the health team member that is essential to the profession.[80] In addition to requiring the observation of data protection laws, Chapter 7 states that professional confidentiality is an

72 Dione Batista Vila-Nova da Silva, Fabio Xerfan Nahas, Rodolpho Alberto Bussolaro, Lydia Masako Ferreira, *Brazilian Plastic Surgery and the Medical Code of Ethics*, Rev. Bras. Cir. Plást. 27(2): (2012), available at **http://dx.doi.org/10.1590/S1983-51752012000200025**; Cléa Adas Saliba Garbin, Artênio José Isper Garbin, Nemre Adas Saliba, Daniela Coelho de Lima, Ana Paula Ayala de Macedo, *Analysis of the Ethical Aspects of Professional Confidentiality in Dental Practice*, J. Appl, Oral Sci. 16(1):75, 75-76 (2008).

73 *Id.*

74 Julio Cesar Namem Lopes, *Medical Confidentiality and the Human Right to Privacy: A Legal Approach*, Revista Bioética 20 (3): 404, 405 (2012). The right to private life is constitutionally guaranteed. *Id.* at 407.

75 *Id.* at 406, 408, 410-11.

76 *Id.* at 408.

77 *Id.*

78 FoxNews, Brazil to Track Numbers of HIV Cases (Dec. 28, 2012), available at **http://latino.foxnews.com/latino/health/2012/12/28/brazil-to-track-numbers-hiv-cases/** (accessed Apr. 1, 2013).

79 *Código de Ética para el Equipo de Salud (2011)*, available at **www.ama-med.org.ar/images/uploads/files/c_etica-ingles.pdf**.

80 *Id.* at chapter 7.

essential ethical duty of health team members and notes that revelation of a patient confidence to even a single person is punishable under the Argentinian Criminal Code. The Code also provides that the confidentiality obligation does not dissolve upon the death of the patient. Under the Code, in cases of pregnancy of an unmarried minor, the physician must remain silent. The Code does, however, permit health team members to disclose health information to a patient's closest relatives, or to others upon the patient's consent. Further, the Code recognizes certain exceptions to the rule of nondisclosure. In particular, "social diseases" of alcoholism, drug addiction, and sexually transmitted diseases must not be disclosed, "provided that this does not represent a real and demonstrable loss to the patient, to a third person, or to the community."[81]

MIDDLE EAST

SAUDI ARABIA

A healthcare ethics code informed by Shariah law, such as in Saudi Arabia, may favor a family-centered or paternalistic approach to disclosure.[82] Data from one survey in Saudi Arabia, for instance, supported the conclusion that 67 percent of physicians and 51 percent of patients surveyed in Saudi Arabia would inform the patient in preference to the family of the diagnosis of incurable cancer. Additionally, 59 percent of surveyed physicians and 81 percent of surveyed patients would inform the patient's family about the patient's HIV status without first obtaining that patient's consent.[83]

ISRAEL

Under Talmudic law, physicians may not share privileged information with their colleagues or anyone else if no benefit to the patient would result therefrom. However, if the maintenance of confidence might cause harm to another person, the latter may be informed. If the individual's right to privacy conflicts with the need of society to prevent harm to others, the prohibitions against tale-bearing and evil gossip are waived and the information must be disclosed to protect others. The disclosure must be factual, accurate, and not exaggerated.[84]

These ethical standards may be reflected in Israel's Patient's Rights Act, 1996, which establishes the rights of every person who requests or receives "medical

81 *Id.*

82 See A. F. Mobeireek et al, *Information disclosure and decision-making: the Middle East versus the Far East and the West*, J Med Ethics 2008;34:225-229.

83 *Id.*

84 F. Rosner, *Medical Confidentiality and Patient Privacy: The Jewish Perspective*, Einstein J. Biol. Med. (2005) 21:81-82, available at **www.einstein.yu.edu/uploadedFiles/EJBM/21Rosner81.pdf**.

care" (defined to include medical diagnostic procedures, preventative medical care, psychological care, and nursing) in Israel.[85] The Act directs healthcare professionals to maintain the dignity and privacy of their patients during all stages of treatment.[86]

Administration of medical care generally requires the patient's informed consent, although an exception may be made in the case of limited circumstances, such as an emergency.[87] If the patient cannot give informed consent, a representative may be appointed to do so.[88] Healthcare professionals must supply patients with "medical information" (i.e., information directly related to the patient's state of physical or mental health, or treatment of such state) to allow the patient to make an informed decision as to treatment.[89] For consent to be truly informed, healthcare professionals should provide medical information to their patients at the earliest possible stage, and in a manner that maximizes the patients' ability to understand the information provided and make free and independent medical choices.[90] However, where facts suggest that the provision of medical information is likely to cause severe harm to the patient's mental or physical health, medical information may be withheld from a patient with approval by an ethics committee.[91]

Healthcare professionals are required to keep "medical records" (defined to include anything documenting medical information) identifying the patient, medical information, and treatment.[92] (Generally, a patient may obtain his or her own medical records unless the information is liable to cause serious harm to his or her physical or mental health or to endanger his or her life.)[93] Subject to certain specified exceptions, healthcare professionals are forbidden to disclose any patient information learned in the course of their duties.[94] Medical information may be disclosed to a third party only if one of the following conditions is met: (i) the patient consents to the disclosure; (ii) the healthcare professional or facility is legally obligated to provide the information (to the government or the like); (iii) the disclosure is made for purposes of the patient's treatment by another healthcare professional; (iv) an ethics committee approves disclosure for the protection of the health of others or the public (and the need for disclosure overrides the patient's interest in non-disclosure); or (v) disclosure is for publication in a medical journal, research, or teaching purposes and all the patient's identifying details are suppressed.[95] Disclosures must be

85 See Israel Patient's Rights Act of 1996 at §§ 1-2.
86 *Id.* at § 10(A).
87 *Id.* at §§ 13(A); 15.
88 *Id.* at § 16(A).
89 *Id.* at § 13(B).
90 *Id.* at § 13(C)
91 *Id.* at § 13(D).
92 *Id.* at § 17(A).
93 *Id.* at § 18.
94 *Id.* at § 19(A).
95 *Id.* at § 20(A).

limited to the necessities of the situation, and healthcare professionals should make every effort to protect the patient's identity.[96] Third parties to whom medical information is disclosed are charged with protecting the dignity and confidentiality of the patient in the same manner as healthcare professionals.[97] All medical facilities must train their staff to prevent inappropriate disclosure of patient information.[98]

ASIA

CHINA

In July 2012, the Ministry of Health for the People's Republic of China issued a "Code of Conduct" to be followed by medical personnel, including hospital management, physicians, nurses, pharmacists, and other staff. A key provision of the Code provides requires such medical personnel to protect patients' rights to informed consent and to keep patient information confidential. Nevertheless, unlike in the West, consent forms for medical treatment are frequently signed not by patients but by their families, a practice recognized in the Republic's social practice and policies.[99] This norm has the potential to breach patient privacy.[100] HIV-positive status in China is highly stigmatized; nevertheless, patients' families are often informed of the diagnosis.[101]

JAPAN

Physicians in Japan, likewise, have historically informed families of diagnoses and prognoses, at times even when patients themselves were not informed of such information.[102] This was particularly true in cases of a highly stigmatized condition, such as HIV or psychiatric disorders.[103] However, such practices are changing, with physicians increasingly engaging in candid discussion of medical information with their patients.[104] On the other hand, failures of the Japanese

96 *Id.* at § 20(B).

97 *Id.* at § 20(C).

98 *Id.* at § 19(B).

99 Jing-Bao Nie, *Medical Ethics in China: A Transcultural Interpretation* (2011), at 142.

100 *Id.* at 144.

101 W. T. Chen, H. Starks, C. S. Shiu, et al, *Chinese HIV-Positive Patients and Their Healthcare Providers: Contrasting Confucian Versus Western Notions of Secrecy and Support*, ANS Adv. Nur. Sci. 30(4): 329 (2007); UN AIDS, The China Stigma Index Report, available at **http://www.unaids.org.cn/en/index/Document_view.asp?id=335**, at 16.

102 Tia Powell, *Cultural Context in Medical Ethics*, Philos. Humanit. Med. (2006), available at **http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1475609/**.

103 *Id.*

104 *Id.*

medical system to maintain patient confidentiality in the case of HIV status have been documented.[105]

AFRICA

The African Charter on Human and People's Rights, or Banjul Charter, which has been ratified by more than 50 countries, omits an explicit right of privacy.[106] However, the right to privacy is reflected in some nations' laws. In South Africa, for instance, patients' right to privacy is recognized in the Constitution, which requires patients' consent to disclose medical records, as well as in medical ethical rules of conduct limiting disclosures of information without patient consent except when required by statute or a court or where justified in the public interest.[107] South African ethical guidelines provide for limited disclosures despite the general recognition of this privacy right; for instance, physicians may, at their discretion, disclose patients' HIV status to partners at risk.[108]

In practice, patient confidentiality in various African countries, such as Uganda, is not always maintained by healthcare workers.[109] But, generally speaking, in Africa, a person's autonomy includes the right to privacy; hospital healthcare workers have an obligation of confidentiality with respect to patient information, diagnosis, treatment, and prognosis of a patient's illness unless the patient has given permission to disclose.[110] Furthermore, because African societies are communal, relatives of a patient may request that healthcare professionals divulge information on the patient's condition, treatment, and prognosis, and a refusal to divulge this information can lead to the patient's being removed by such relatives from the hospital.[111]

Indeed, in some nations, competing interests may limit patients' right to privacy. Ubuntu is the central concept of social and political organization in African philosophy, particularly among the Bantu-speaking peoples of Sub-Saharan

105 Kenneth Kipnis, Medical Confidentiality, in The Blackwell Guide to Medical Ethics, (Rosamond Rhodes, Leslie P. Francis, and Anita Silvers, eds., 2007), at 121.

106 Michelo Hansungule, *African Courts and the African Commission on Human and Peoples' Rights*, in African Courts and the African Commission on Human and Peoples' Rights, 233, 259.

107 Health Professions Act 56: Ethical Rules of Conduct for Practitioners Registered under the Health Professions Act of 1974, available at **http://www.hpcsa.co.za/conduct_rules.php**.

108 Health Professions Council of South Africa, *Guidelines for Good Practice in the Health Care Professions: Ethical Guidelines for Good Practice with Regard to HIV* (May 2008), § 9, available at **http://www.hpcsa.co.za/conduct_generic_ethical_rules.php**.

109 KC Team, *Breaching Patient Confidentiality: a Common Cause of Stigma in Uganda*, at **http://www.keycorrespondents.org/2010/11/09/breaching-health-confidentiality-a-common-cause-of-stigma-in-uganda/**.

110 Robert M. Veatch, *African Ethical Theory and the Four Principles, Cross-Cultural Perspectives in Medical Ethics*, 2d ed. (2000), at 252-53.

111 *Id.*

Africa; it consists of the principles of sharing and mutual caring.[112] "The Ubuntu worldview has been recognized as the primary reason that South Africa has managed to successfully transfer power from a white minority government to a majority-rule government without bloodshed."[113] Under the concept of Ubuntu, "a person is a person through other persons," a concept based on such values as humanity, caring, respect, compassion, and "ensuring a happy and qualitative human community life in a spirit of family."[114] Given these values, personal privacy may be subordinated in some cases to communal interests.[115]

112 Rafael Capurro, ed., et al, *African Information Ethics in the Context of the Global Information Society*, Int'l Rev. Info. Ethics, No. 7 (Sept. 2007), available at **http://www.i-r-i-e.net/1-15.htm**.

113 *Id.* (citations omitted).

114 *Id.* (citations omitted).

115 *Id.* (citations omitted).

CASE STUDIES FROM SELECT JURISDICTIONS IN AFRICA, ASIA, AND LATIN AMERICA

This section of the paper takes a closer look at the state of privacy law and any particular legislation and policy in the mHealth space in a select group of jurisdictions that have experienced significant growth in the adoption of mHealth products and services. We conducted a high-level gap analysis in consultation with local privacy attorneys in Tanzania, Uganda, Nigeria, Bangladesh, India, Peru, and Chile. The results of this analysis are summarized in this section.

BANGLADESH

In Bangladesh, there is no specific data protection law or privacy law that specifically applies to mHealth. In addition, Bangladesh has not implemented specific laws that govern the use and disclosure of health and medical data in general (i.e., an omnibus health data law similar to HIPAA in the United States).

Certain protection for medical data (which would encompass certain types of mHealth data) is provided by the medical ethics rules established by the Bangladesh Medical Association ("BMA"). The Medical Practitioners Act does not provide for any secrecy of information or data protection or communication, but physicians are accredited under BMA, and they are bound by its codes and declarations. Under such rules, patient-specific medical data may be disclosed only to the patient except in certain specified situations, such as where there is a possibility of adverse effect on the medical condition of a patient. Strict secrecy is maintained over patients' files, and relevant consents must be sought for information sharing when relevant. Note, however, that amalgamated and aggregated data are used routinely by laboratories and researchers on an anonymous basis.

In addition to the protections established by the BMA, there are other, more general privacy protections established by Bangladeshi law that could apply to mHealth depending on the context:

- The Information & Communication Technology Act provides perhaps the strongest general protection for mHealth data because it applies to any information stored electronically and prohibits unauthorized disclosure of

personal data stored in such electronic format without the relevant consent of the individual. Violations are subject to imprisonment and/or fines.

- The Bangladeshi Constitution establishes a general right of privacy in correspondence and communications that presumably could be applied to health-related communications. Civil claims for damages may be imposed for violations of the right.
- The Consumer Protection Act prohibits the unauthorized disclosure of personal data of consumers resulting in adverse consequences to the consumer. In addition general rules for loss and damages against any breach of contract/unlawful activities would be included. Violations are subject to imprisonment, fines, or both.

As a possible limitation on the right of privacy in communications including communications related to mHealth, the Bangladesh Telecommunications Act provides the Bangladeshi government the right to empower any of its agencies to record, prevent and collect information regarding communications made by any person through telephone for the purpose of protecting the security of the state and public tranquility. In order to administer this law, the Bangladeshi government can require the assistance of a service provider in the recording, blocking or collecting of the information at issue.

In Bangladesh, healthcare workers are bound by ethical codes and the law to maintain the confidentiality of their patients' health information where the patient has not consented to the disclosure; even family members are not to be given information about a patient's medical history.[116] But again, concern for the safety of others may warrant disclosure.[117] This is of particular concern where certain conditions, such as HIV status, are heavily stigmatized.[118]

CHILE

There is currently no law in Chile related specifically to the regulation of mHealth or related data. The Chilean Penal Code (*Código Penal*) requires that civil servants or professionals who reveal personal information be imprisoned and fined, while the Chilean Penal Procedural Code (*Código Procesal Penal*) compels health professionals to report any fact that may constitute the breaking of a law.[119]

Chilean Law No. 20.584 regulates the rights and obligations of people with regard to actions connected to their health service (the English translation of the law is, "The rights and obligations of people in regards to actions connected

116 Mohammad Waseem Khan, *Breach of Confidentiality: Unintentional Common Practice Due to Misunderstanding and Unawareness*, Bangladesh J. Bioethics 2(3) (2011).

117 *Id.*

118 Md. Tanvir Hasan, Nabila S. Khan, Owasim Akram, et al, *Experiences of Discrimination among People Living with HIV/AIDS in Bangladesh*, Asia J. Pub. Health, 3(2): 44, 44-45 (2012).

119 C. Olivari, Maria Teresa Muñoz Sastre, Myriam Guedj, et al. *Breaking Patient Confidentiality: Comparing Chilean and French Viewpoints Regarding the Conditions of Its Acceptability, Universitas Psychologica*, 10(1):13, 14 (2011).

to their health service" or "ROHSL"). Under ROHSL, all information related to the clinical record of a patient and the studies and other documents wherein procedures and treatments are registered about a patient will be considered "sensitive data" under the Chilean data protection law (discussed below) and subject to the related protections, including the obligation to obtain consent to collection and disclosure and to secure such information electronically.

Moreover, each health center in Chile, whether an outpatient center, hospital, or clinic, must clearly and visibly exhibit a "Charter of Patient Rights and Responsibilities" in addition to a book or other form for registering complaints. If a patient is not satisfied with a response, he or she may refer the matter to the Superintendent of Health. In addition, among the principal patient rights, the new law (enacted in October 2012) states that every person, irrespective of the healthcare provider, is entitled to receive the relevant healthcare services promptly and without any arbitrary discrimination, along with dignified treatment, spiritual company and assistance; comprehensible information on the diagnosis, treatment, and medication; and *reservation of the clinical record*.

ROHSL establishes the obligation for institutional providers, both public and private, to maintain an updated database and to make the records stored therein freely accessible (to the relevant individuals). The available information should include information about costs of services, supplies, and medication.

Health centers with a high number of indigenous clients must have facilitators who speak the indigenous language. The centers also must provide signs in the corresponding language as well as in Spanish.

ROHSL also sets out responsibilities for patients, including obligations to provide truthful information regarding identity, address, and sickness; to treat health staff with respect; to take care of the health center's facilities and equipment; to respect the internal rules of the establishment as well as the certificate of their medical information; to be informed about facility's hours of business, types of service, and forms of payment in force; and to become informed about the established procedures for lodging complaints and consultations.

Penalties for violation of ROHSL include penalties for violations of the data privacy law (see below). Violations would generally be assessed against public healthcare providers and medical practitioners (physicians).

Chilean Law 19.779 specifically protects the confidentiality of a patient's HIV status, requiring health professionals who analyze fluids and communicate the information to maintain strict confidentiality.[120]

Chile has also implemented the Code of Ethics of the Medical Association of Chile ("CEMAC"), which applies to all medical practitioners (physicians) who are members of the Medical Association of Chile. Note, however, that membership in this association is not mandatory for practitioners. For members, CEMAC

120 *Id.*

requires that all heath practitioners ensure the confidentiality of all information that stems from professional services. This confidentiality duty also extends to all documentation in which clinical data, diagnosis, and prognosis are registered. Penalties for violation include a warning, censorship, a fine, suspension, ineligibility to hold union position, and expulsion from CEMAC. Confidentiality may be appropriately and ethically breached in limited cases, most notably upon the diagnosis of certain illnesses, such as syphilis, that are required by law to be reported to the authorities, or in the case that disclosure is necessary in order to avoid severe harm up to the patient or others.[121] The determination of whether such breach is legitimate is complex and will typically involve several decision-makers. [122]

A survey study of Chilean nationals supported the conclusion that 70 percent of healthcare professionals and 77 percent of laypersons believed that the following factors were relevant to breaking confidentiality in the event a husband might transmit a serious sexually transmitted disease to his wife: (a) the patient's intention to adopt protective behavior, (b) the patient's intention to inform the spouse, (c) the severity of the risk (i.e., of the consequences of acquiring the disease), (d) the physician's consultation with an expert, and (e) the time taken to discuss the severity of the disease with the patient. Data from a recent survey study supported the finding that most Chilean physicians believe that breaching patient confidentiality may be acceptable in some cases, a view that is consistent with the official position of the Chilean ethical code (and the ethical codes of nations such as the United States and the United Kingdom).[123]

Due to their broad application to data contained in and related to patient records, the confidentiality and related obligations of ROHSL and CEMAC would extend to mHealth and related data so long as such data relates to an actual patient record or other information covered by ROHSL and CEMAC.

In addition to the restrictions that apply specifically to health and medical data, Chile has enacted an omnibus data privacy law, the protections of which apply to all personally identifiable data, including health data. The data protection law imposes requirements to provide notice to individuals and in certain circumstances obtain their consent regarding the use and disclosure of their personal data as well as requirements regarding providing adequate security to personal data and the like. In addition and as discussed above, this data privacy law provides special protections to "sensitive personal data", which includes health and medical data. Such special restrictions impose consent requirements on the collection, processing, and disclosure of such sensitive data. There are no provisions in the data privacy law that set special protection for women, minors

121 *Id.*

122 *Id.*

123 *Id.* at 23.

and spouses, or family members. However, on January 11, 2012, a bill, which has not yet been enacted, was entered by the Chilean Congress to update the data privacy law to ban the use of private/sensitive data of children except for data indispensable for identification purposes or in the case of a medical emergency (which would still require parental consent).

Courts can order the correction, blockage, or deletion of data from the database and impose a fine for violations of the data privacy law. Violations are also subject to civil claims for damages.

INDIA

In India, there is no specific law governing health and medical data (i.e., an omnibus health data law similar to HIPAA in the United States).

Nevertheless, protection for health and medical data (which would encompass mHealth data) is provided by the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 ("MCI Code"). The MCI Code applies to Registered Medical Practitioners in India (registered with various state medical councils as a precondition to practice medicine) and requires physicians to refrain from disclosing any "secrets of patients" that have been learned in the exercise of the physician's profession (subject to certain limited exceptions, such as where required by applicable law and/or where necessary to prevent the spread of communicable diseases). In addition to general health data, there are two types of confidential information that a physician is prohibited from disclosing: (1) information concerning individual or domestic life of patient observed during medical attendance; and (2) information concerning defects in the disposition or character of patients observed during medical attendance. In case a medical practitioner is found to have failed to observe any of the duties prescribed in the MCI, such violation is considered to be an act of professional misconduct and the practicioner can be subject to a penalty ranging from temporary suspension to permanent disqualification from the practice of medicine. This penalty is in addition to any other criminal or civil liability that may be incurred for disclosure of patient information.

In addition, India has also enacted the Information Technology Act, 2000 (the "ITA") and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Data Privacy Rules"). Although the ITA and the related Data Privacy Rules are not directed specifically at health and medical data, the majority of their protections, particularly the consent and disclosure requirements, apply to "sensitive personal data" as defined by the Data Privacy Rules. The definition of sensitive personal data expressly includes physical, physiological, and mental health

condition, sexual orientation, and medical records and history. The ITA and the Data Privacy Rules also impose significant information security requirements on individuals and entities that hold sensitive personal data and require such entities to develop and post (generally on a company website) a comprehensive privacy policy and to appoint a grievance officer. All such requirements would apply to mHealth data (so long as it meets the definition of sensitive data). Violations of the ITA and Data Privacy Rules are subject to fines and imprisonment as well as civil claims for damages.

The Mental Health Act, 1987, permits governmentally authorized officers to inspect psychiatric hospitals, to demand records, and to interview patients. Indian case law recognizes the right of clinicians to disclose patients' HIV status to their would-be partners (i.e., a fiancé) on the basis that the public interest prevails over the duty of confidentiality owed by a physician to a patient.[124]

From a cultural perspective, India has a very close-knit family system. Many households comprise both immediate and extended family members. Any sensitive personal data received from family members would also be protected by the ITA and the Data Privacy Rules.

A patient in India has a general right of privacy under the 2002 Medical Council of India Code of Ethics Regulations; however, confidentiality may be breached where required by law or if necessary to ensure public safety (e.g., for prevention of crime or disorder, for protection of health or morals, for protection of rights and freedom of others, for purposes of registering certain diseases, for investigating communicable diseases, or for reporting adverse drug events).[125] In addition, patients must obtain a disability certificate in order to access benefits under the nation's disabilities act, which could jeopardize health information privacy by placing it in the government's control – particularly for those with psychiatric conditions.[126]

NIGERIA

There is currently no law in Nigeria specifically related to the regulation of mHealth data. However, the national medical ethics code contains specific obligations related to the provision of mHealth services.

124 Natasha Vaz, *Health Privacy in India: A Legal Mapping*, available at **http://staff.science.uva.nl/~noordend/wees/2012/vaz.pdf**.

125 *Id.*

126 *Id.*; see also N. N. Mishra, L. S. Parker, V. L. Nimgaonkar, et al, *Disability Certificates in India: A Challenge to Health Privacy*, Indian J. Med. Ethics, 9(1): 43 (2012).

The Medical and Dental Council of Nigeria has issued a Code of Medical Ethics (the "Code") pursuant to a mandate set forth in Nigeria's Medical and Dental Practitioners' Act (Cap. M8, Laws of the Federation of Nigeria, 2004), which establishes protections for medical and health data. The Code applies to all medical and dental practitioners and provides that all communications between a patient and a medical or dental practitioner made in the course of treatment are confidential and cannot be disclosed unless compelled by law. Medical and dental practitioners may disclose such communications upon receiving informed, express consent from the patient. The consent must be in writing. The Code provides that next of kin should give consent for patients who are minors, are unconscious or who have a mental impairment. Failure to obtain consent is deemed to constitute professional negligence on the part of a practitioner, who has a duty of care to each patient under the Code. In addition, the Code requires that practitioners clearly inform patients of the benefits and risks of any procedure.

NIGERIA'S ETHICS CODE HAS PROVISIONS SPECIFIC TO mHEALTH

The Code contains particular provisions related to telemedicine, requiring that practitioners make appropriate arrangements to maintain the security of patient personal information when that information is stored, sent or received by fax, computer, email, or other electronic means.

The Code contains particular provisions related to telemedicine, requiring that practitioners make appropriate arrangements to maintain the security of patient personal information when that information is stored, sent, or received by fax, computer, email, or other electronic means. These provisions would be particularly applicable to mHealth. Where a practitioner fails to abide by the obligations for patient privacy and confidentiality, the practitioner faces penalties.

In addition to the obligation to obtain patient consent for disclosure of communications between patient and practitioner, Sections 37, 45 and 46 of the Constitution of the Federal Republic of Nigeria (the "Constitution") establish a general right of privacy for Nigerian citizens. This right of privacy under the Constitution covers individual correspondence, and telephonic and telegraphic communications. Therefore, collection and disclosure of an individual's personal information, including health information, may constitute a violation of the Constitutional right of privacy, unless the individual has provided express consent. Pursuant to this constitutional right of privacy, an mHealth service provider would be obligated to obtain consent for the collection and transfer of individual data. Individuals whose privacy rights have been violated may bring a claim for enforcement in the state or federal high court.

PERU

There is currently no law in Peru related specifically to the regulation of mHealth or related data. Peru has, however, enacted Law No. 26842, General Health Law ("GHL").

Subject to certain limited exceptions, GHL prohibits the release of information regarding a medical act (information related to the actions taken by the doctor and revealed by the patient for the purposes of treatment) without written consent. Doctors are also obligated to provide a copy of medical records to patients upon request, and GHL requires that medical records be subject to appropriate security and confidentiality controls. GHL also establishes that disabled people, children, teenagers, mothers, and elderly people who have been abandoned must receive priority attention.

A health professional, technician, or assistant who provides or discloses, by any means, information related to a medical act in which he or she participates or of which he or she has knowledge can incur civil or criminal liability, as appropriate, without prejudice to the sanctions that may be imposed by ethical codes. The following administrative penalties may also be imposed: admonition, fine, or temporary or permanent closure of the healthcare facility.

Peru has also implemented the Ethics and Deontology Code of the Peruvian College of Physicians, which establishes confidentiality requirements for patient data. Physicians found to violate this Code may be subject to the following sanctions: (1) note of reprobation; (2) private admonition; (3) fine; (4) public admonition; (5) suspension from practicing medicine for a maximum of two years; and (6) expulsion from the medical college.

Due to their broad application to data contained in and related to patient records, the confidentiality and related obligations of GHL and the code of ethics would extend to mHealth and related data (so long as such data relates to an actual patient record or other information covered by GHL and the code of ethics).

In addition to the restrictions that apply specifically to health and medical data, Peru has enacted Law No. 29733, Personal Data Protection Law, an omnibus data privacy law, protections of which apply to all personally identifiable data, including health data. The data protection law imposes requirements to provide notice to individuals and in certain circumstances obtain their consent regarding the use and disclosure of their personal data as well as requirements regarding providing adequate security to personal data and the like. In addition and as discussed above, this data privacy law provides special protections to "sensitive personal data", which includes health and medical data. Such special restrictions impose consent requirements on the collection, processing, and disclosure of such sensitive data. Exceptions to the consent requirements with regard to health data apply under the law when collection and processing are

necessary in a situation of risk, prevention, diagnosis, or medical or surgical treatment of the owner of the information, if such processing is carried out by a medical institution or by health professionals, complying with the professional secret, for public health reasons, or for the realization of epidemiologic or analogous studies.

Note also that regulations for the data protection law have not been enacted, but it is anticipated that such regulations will establish special treatment for the processing of personal data of children and teenagers.

Violations of the personal data law trigger monetary fines.

TANZANIA

Tanzania has no specific and comprehensive privacy legislation that applies to mHealth or otherwise. In addition, Tanzania has not implemented specific laws that govern the use and disclosure of health and medical data in general (i.e., an omnibus health data law similar to HIPAA). Tanzania has, however, enacted several laws intended to protect the confidentiality and security of certain types of information. For example, the HIV & AIDS (Prevention and Control) Act of 2008 applies specifically to prevention, treatment, care, support, and control of HIV and AIDS. At a high level, this act prevents healthcare practitioners from disclosing (without patient consent) records and documents related to HIV and AIDS (e.g., test results).

Similarly, the Human DNA Regulation Act of 2009 applies to Human DNA or genetic information of any person and generally sets out the requirements for the collection, disclosure, protection, transport, destruction, and related treatment of such DNA or genetic information.

Both the HIV & AIDS (Prevention and Control) Act of 2008 and the Human DNA Regulation Act of 2009 are generally technology-neutral and would apply mHealth applications and activities to the extent they involve the relevant covered information (and the individuals covered by such acts).

Tanzania has also established the Guiding Principles on Medical Ethics and Human Rights in Tanzania (Code of Ethics of Medical Profession in Tanzania), which, among other provisions, contains confidentiality provisions for patient data.

Apart from the laws and code of practice discussed above, there are other laws that relate to health information, such as the Medical Practitioner and Dentists Ordinance of 1959. However, most of the laws that deal with health information in Tanzania cover only to confidentiality of the data and not broader privacy concerns.

Outside the realm of protections for health data, the Electronic and Postal Communications Act, Act No. 3 of 2010, deals with confidentiality in electronic communications in Tanzania. This Act, which could apply to health data as well as other types of data, imposes the duty on electronic service providers to secure confidentiality of such communications. In addition, Article 16 of the United Republic of Tanzania Constitution of 1977 provides for a general right to privacy.

UGANDA

In Uganda, there is no specific data protection law or privacy law that directly applies to mHealth. In addition, Uganda has not implemented specific laws that govern the use and disclosure of health and medical data in general (i.e., an omnibus health data law similar to HIPAA).

Uganda has established the National Guidelines For Research Involving Humans as Research Participants (2007) (the "Research Guidelines"), the protections of which apply to all research participants and related data collected from such participants. At a high level, the purpose of the Research Guidelines is to ensure that all research in which humans participate as research subjects is done ethically, mindful of injury to participants and to ensure that the research data collected is kept confidential. The privacy/confidentiality protections of the Research Guidelines are broadly worded to protect the privacy of participation during and after the research and the confidentiality of data collected during the research.

Ugandan law does recognize the right to privacy as a human right.[127] Ethical and legal policies for the protection of health information are generally not well developed.[128] Additionally, healthcare providers often struggle to balance a duty to notify partners at risk with a competing ethical obligation to protect the medical confidentiality, safety, and well-being of people who have HIV.[129] Special protections are provided to certain groups, including children, mature and emancipated minors, street children, prisoners, the homeless, substance abusers, people with disabilities, armed forces personnel and pregnant women. The Uganda Ministry of Health has promulgated a National Health Services Laboratory Policy that requires laboratory staff to safeguard privacy and confidentiality.[130]

---

127 Electronic Privacy Information Center, Uganda Privacy and Human Rights Report 2006, available at **http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-31.html**.

128 Kato Mivule, Claude Turner, *Applying Data Privacy Techniques on Published Data in Uganda,* Int'l Conf. e-Learning, e-Bus., EIS, and e-Gov, available at **http://www.google.com/url?sa=t&rct=j&q=%22privacy%20in%20uganda%22%20health%20medical%20ethics&source=web&cd=16&ved=0CDsQFjAFOAo&url=http%3A%2F%2Fworld-comp.org%2Fproc2012%2Feee%2Fpapers.pdf&ei=9dqJUYDvOMep0AXnwoDgBQ&usg=AFQjCNFd85LDO9mzgmgEL_DWWEy9mxUoaA**, at 110.

129 Carla Makhlouf Obermeyer, Sarah Bott, Ron Bayer, et al. *HIV Testing and Care in Burkina Faso, Kenya, Malawi and Uganda: Ethics on the Ground*, BMC Int'l Health and Human Rights 2013, 13:6 (2013), available at **http://www.biomedcentral.com/1472-698X/13/6.**

130 Uganda Ministry of Health, *Uganda National Health Laboratory Services Policy*, available at **www.umltaug.org/policy.pdf**, at 12.

WORKING TOWARD AN mHEALTH PRIVACY LAW FRAMEWORK

We have now set forth a more informed context for addressing mHealth data privacy and security issues through the law by sketching out the forces and actors at play in the mHealth ecosystem, by identifying some of the competing interests at play and their interrelatedness, and by attuning the reader to the complexity of legislating data privacy and security regulations. We learned that any effort at legislative reform to address mHealth privacy and security concerns must first take stock of the cultural, technological and legal context at play and acknowledge the effect that these and other factors could have on mHealth privacy and security and the success of any new policies.

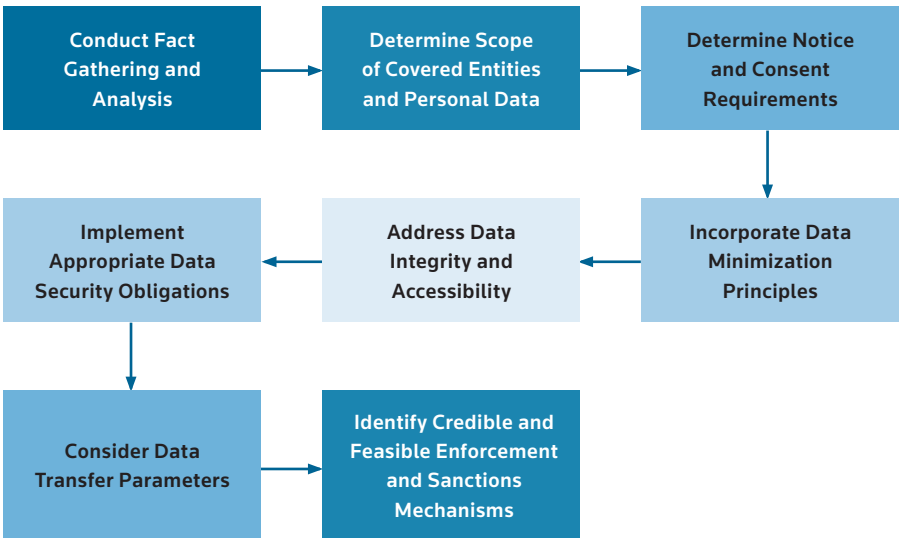
We have also outlined the current state of data privacy and security laws around the world in all of its diversity and breadth, from the sectoral approach in the United States to the omnibus approach in Europe and those that fall in between. We aimed to simplify that diversity for purposes of comparison and study by stripping the laws down to their common core elements: scope of coverage, notice and consent provisions, onward transfer restrictions, data security, retention, integrity and availability, and enforcement. Some of these national laws also impose registration requirements and the appointment of dedicated data protection officers within covered organizations, but these requirements are aimed at providing further oversight and not the essence of providing privacy assurances to individuals. As such, these types of legal restrictions were not covered in detail. We learned through this exercise that mHealth has not been specifically addressed in any national law but that many existing laws are sufficiently broad in their application so as to reach mHealth products and services that handle covered data (either through specific health privacy laws or omnibus privacy laws). These laws also provide examples to those countries that have yet to develop omnibus or specific health privacy laws. However, further analysis should be conducted into the effectiveness of these laws given their current scope and any areas for potential reform.

Next, we looked at various examples of medical ethical codes around the world for lessons that could be applied to the mHealth context and to better understand the baseline privacy protections already afforded to patients in certain parts of the world. In many ways, these ethical codes both inform and reflect the national concept of health privacy and could provide a roadmap to future mHealth policies and legislation.

Finally, we reviewed country law summaries, developed in collaboration with local attorneys in Chile, Peru, Uganda, Nigeria, Tanzania, India and Bangladesh to assess where privacy law stands in some of the countries with the most promising adoption of mHealth solutions and services. Among these countries only Peru and Chile have comprehensive data protection laws. India and Bangladesh have other laws that address data privacy and security in certain respects. And, neither Uganda, Tanzania nor Nigeria have specific privacy laws but do provide some baseline protections through their constitutions and/or medical ethics codes. Further study should be conducted as to the rates of mHealth adoption in these countries and any correlation with the degree of privacy regulation to better understand how the law can help more users take advantage of mHealth's benefits.

Aided with this information, we can now begin shaping a framework to guide the mHealth community as it addresses privacy and security concerns in the effort to bring mHealth to scale. For this purpose we will use the core shared principles present in existing privacy laws and set forth some key guidelines and considerations to take into account when deciding where to draw the line under each category.

Figure 5. A Framework for Assessing Privacy Law Policy Issues



FACT GATHERING AND ANALYSIS

Given the complexity, multiplicity of actors and highly culture-specific dimension of privacy, consideration of mHealth privacy and security law issues should begin with a robust fact-finding exercise. This step should engage key stakeholders from the mHealth ecosystem (see Figure 4, above) and take into account the national legal framework, sophistication of institutions, technological infrastructure, enforcement resources and general culture of respect for the law. Unique vulnerabilities should be noted (such as entrenched norm of discussing patient information among healthcare staff outside of delivery of care context, which was identified in discussions with country health ministry representatives at the start of this project) and highlighted. Existing constitutional, ethical and industry-developed privacy protections should be identified so as to provide a baseline from which reform can begin to take shape. Finally, the particular mHealth uses in operation and likely to be implemented should be taken into account.

The result would be a high-level map of the data flows related to mHealth in a particular jurisdiction, the likely data recipients (and their location), those who would seek access to the information (and their location) and the places where the privacy and security of such information may be especially vulnerable. Enforcement capabilities and resources would be identified and mapped to the greatest identified vulnerabilities. An earnest understanding of current local technological infrastructure would be kept front and center during the entire discussion. Only after completing this exercise, should a review of model laws and approaches be undertaken and the business of considering new laws begin. Otherwise, policymakers may risk adopting foreign approaches that are not compatible with local capabilities and contexts.

DETERMINING SCOPE OF COVERAGE

Taking into account the results of the fact-gathering exercise, policymakers should consider the reach of the new laws. How will jurisdiction be exercised? What party in the mHealth supply chain will have primary responsibility for ensuring compliance with privacy and security regulations? Will they be explicitly required to demand the same level of accountability from their own providers and affiliates? Where is this burden most efficiently placed? Where is it most likely to produce a compliant culture? What explicit exceptions should be made?

From the examples of current legislation we have reviewed, most place responsibility at the first point of data collection. This has many benefits, most important of which is the closest relationship between the data subject and the data collector. This proximity could facilitate better privacy disclosures,

better understanding of the data subject's privacy expectations and greater accountability from a market perspective (the primary service provider is more likely to hear of a complaint than a distant subcontractor). However, many existing laws have found the need to extend at least a subset of privacy and security regulations to other participants in the supply chain. Examples include HIPAA, which was amended to require covered organizations to extend by contract certain HIPAA obligations to service providers that could have access to covered data and to bring such entities into HIPAA's jurisdiction for purposes of enforcement. More recent revisions added two new categories of covered entities, Health Information Organizations (which provide data transmission services for covered data) and Personal Health Record Vendors (which provide individuals with a data storage solution for their personal health records). Several U.S. states also have required that data security standards be contractually-mandated down the data management supply chain. These legislative changes reflect a change in the health information business models in existence and new ways of transmitting and storing covered data. They are also a response to new perceived vulnerabilities in the eHealth ecosystem. These are the types of considerations that should inform continued reform in this area.

In sum, the following are some of the key issues that should be addressed when determining scope of coverage:

- Jurisdictional reach (persons/entities with a local presence or also those who store or process data of residents but have no local presence)
- Persons/entities obligated to comply (primary data collectors or also other service providers who may have access and/or provide data storage and processing functions)
- Definition of "Personal Information" (any information that can be linked to an individual or more discrete categories of data, such as health information, that deserves special protection)
- Exceptions (for use of aggregated data for public health purposes, biomedical research, national emergencies, etc.).

NOTICE AND CONSENT (CHOICE)

For individuals to have the practical ability to exercise control over the collection, recording, access, and dissemination of their mHealth Data, they must be adequately informed about these practices and provided a choice. Current legislation addresses this core principle through disclosure and consent requirements. Most jurisdictions with specific health privacy or comprehensive privacy legislation require affirmative opt-in consent prior to the collection or use of sensitive categories of data, such as personal health information, for

uses other than delivery of care, healthcare operations, payment and research based on de-identified data. For other types of information, such as name and contact details, some jurisdictions require only notice and opportunity to object, also referred to as tacit consent. A minority of jurisdictions require affirmative consent prior to collection of any type of personal information.

When it comes to required disclosures, most jurisdictions provide a representative list of the types of information that must be included in an effective privacy notice but do not prescribe specific disclosure language and leaves that to the disclosing entity. This can be beneficial because it is likely to lead to more tailored disclosures that are more specific to the particular service and data usage than a boilerplate disclosure. Some laws provide only a standard that disclosing entities must meet, such as clear and accurate (the FTC Act in the United States, as applied to privacy disclosures), which is usually applied to more generic collections of information rather than sensitive information, such as personal health information.

Given the options outlined above, determinations as to the type of notice and consent requirements should involve consideration of:

- Whether all personal information will be treated the same or whether certain categories of sensitive personal information will trigger greater compliance obligations
- Whether to require affirmative opt-in consent for changes in the usage of personal information collected (from its original disclosed purpose)
- Benefit of requiring a comprehensive list of disclosure categories against the transactional cost to individuals of reading and processing such disclosures for every type of personal information collection
- Feasibility of obtaining affirmative consent via electronic processes, potentially requiring corollary changes to laws of evidence making electronic consents admissible in court (to prove that an individual indeed consented to the described privacy practices). Where affirmative consent is required, covered entities should be provided with clear and practical methods for obtaining such consent. Uncertainty in this area may discourage compliance or even entrance into certain markets with particularly cumbersome or arcane requirements
- What degree of notification is required to provide individuals with the ability to exercise informed consents vs. encouraging covered entities to provide a laundry-list of potential uses (to over-comply where the line is unclear). Over-disclosure runs the risk of confusing the individual and may cover remote risks that trigger trepidation rather than trust
- For populations with significant rates of illiteracy, what alternatives can be employed to ensure effective communication of the disclosures and ability to evidence consent so that legal notice and consent requirements do not create a barrier to providing services to these populations

– Whether a simplified approach to notice and consent should be adopted whereby only secondary purposes (i.e. purposes other than treatment, payment, healthcare operations, and de-identified research) would trigger notice and consent obligations.

DATA MINIMIZATION

The rise of electronic communication has correlated with an explosion in the amount of data that is created, and increasing computing power has allowed for much more of that data to be stored. Despite this, privacy law continues to champion the concept of data minimization and with good reason. The more data that is collected and stored, the more risk that is created (no matter the practices and standards built around collection and storage). Further, broad collections of personal information also make it more challenging for individuals to keep tabs on the uses and disclosures of such information, compromising their ability to exercise control over how their personal information is handled.

Data minimization (sometimes also referred to as "Privacy by Design" or "Purposeful Data Collection") refers to the reduction of irrelevant data collections, uses, and transmissions. Just because an mHealth application may provide a cheap and easy way to gather and organize enormous amounts of personal information, this does not necessarily mean that it should be done. There should be a defined purpose for each collection of personal information, especially in the case of sensitive information such as personal health information.

Most laws do not address this issue head-on but attempt to encourage data minimization by requiring covered entities to use personal information only for the purposes collected and appropriately disclosed. The obligation to account for all personal information in this manner naturally drives covered entities to limit the amount of data collected (and, thus, reduce their compliance burden and regulatory exposure).

However, this principle should be weighed against the potential benefits of "big data" especially in the healthcare field. There are countless initiatives around the data-driven healthcare movement, which promises, among other things, to create more tailored and effective treatment by leveraging large data stores to more accurately predict outcomes and determine successful treatment avenues.[1] Some proponents say that the additional value of big data is that it could lead to discoveries and innovations that no one has currently envisioned or set out to find.

1 *See*, e.g., McKinsey & Co., *The 'big data' revolution in healthcare: Accelerating value and innovation* (Jan. 2013).

This is precisely why limiting the uses of data for privacy purposes could curtail the effectiveness of certain big data projects in the healthcare field. It is not always clear at the outset which data sets will prove important. For this reason, it may be appropriate to create exceptions in the privacy laws for valid research purposes (perhaps with a clear application and approval structure administered by a public health authority) and for the use of anonymized or aggregated data. Of course, individuals are always free to participate in such initiatives and provide their data voluntarily. However, it may still make sense to bind these entities to comply with specific data security obligations even if the notice and consent requirements may be relaxed for these limited purposes.

DATA INTEGRITY AND ACCESSIBILITY

Any personal information collected should be accurate and should remain accessible to the data subject for the purposes of updating and correcting. When personal information is stored out of the data subjects' reach, the risks associated with errors in their records are compounded, particularly in the healthcare context. Payors and providers are likely to rely on these records to make decisions about treatment and payment of services, so that errors could have a substantial impact on the data subject. This principle also is key for securing the individual's ability to exercise control over the collection, recording, access, and dissemination of their mHealth Data. Access and the ability to correct records is instrumental to the concept of control.

Most laws, therefore, require covered entities to provide data subjects with access to their personal information in some shape or form, especially sensitive information such as personal health information. Some require covered entities to provide data subjects with an accounting of all personal information stored (the more personal information that is regulated / the broader the definition of personal information, the more burdensome this requirement), while others require transmission or access to a copy of that subject's personal record. Complying with such obligations requires covered entities to implement special data collection and organization controls and to make structural changes that allow the personal information of one data subject to be accessed without accessing the personal information of others. Therefore, these types of provisions are difficult to enact with retroactive or immediate effect. The cost of compliance should be considered carefully along with limitations on vexatious or abusive requests by data subjects. Most legislation allows covered entities to take "commercially reasonable" measures to respond to such requests and allow a reasonable time to respond.

Legislation with respect to data access and correction should also take into account the following issues:

- If someone has healthcare power of attorney for an individual, can they obtain access to that individual's medical record
- Can the personal representative of an adult or emancipated minor obtain access to that individual's medical record
- How can family members of a deceased individual obtain the deceased individual's personal health information that is relevant to their own healthcare
- Do parents have the right to see their children's medical records
- If a child receives emergency medical care without a parent's consent, can the parent obtain all information about the child's treatment and condition
- Will this access and correction obligation be extended beyond the primary data collector? Will it apply to research uses as well
- Will individuals have access to their records at no cost

Maintaining the accuracy and integrity of personal information stored is also crucial and depends on sufficient internal controls to keep the data secure. This principle is discussed in the next section.

DATA SECURITY

Data security is non-controversial in that most jurisdictions agree that it is essential to a privacy law system, especially in the digital, globalized age. However, they have approached the issue quite differently. The United States is one of the legislative leaders in this area, with some of the broadest, most detailed and most punitive data security laws on the books. Under U.S. law, data breaches trigger significant notification obligations and could lead to considerable fines. As noted above, data security obligations are more likely to be regulated all the way through the data management supply chain than privacy obligations.

On the opposite side of the token is Europe with very robust and exacting privacy laws but very few member states with any specific requirements as to data security or measures to be taken in case of a security breach.

Policymakers considering legislation on data security should consider:

- In how much detail will data security be regulated? Where is delegation to industry standards appropriate? How can the law remain flexible and relevant with changing security threats and solutions
- Whether to include specific data retention provisions or require covered entities to simply keep data no longer than is necessary and employ secure disposal measures

- Whether specific identity and age verification practices should be legislated across the board or just for particularly sensitive data (such as online collection of children's data under the COPPA in the United States); if so, what practical verification options will be offered to covered entities? Uncertainty in this area can be especially frustrating and discouraging to covered entities
- Whether to institute data breach notification obligations on covered entities, their sub-contractors, those with a local presence or any that store residents' data

DATA TRANSFERS TO THIRD PARTIES AND ACROSS BORDERS

Restrictions on the ability to transfer personal information from the original data collector to third parties and beyond the data subject's home country aim to ensure that the privacy disclosures made and the protections offered at the point of collection hold throughout the lifecycle of the data collected. Especially in mHealth, a number of entities are likely to process, store or access a data subject's personal information, and many of these entities may be located in multiple countries. To the extent that these entities are completely divorced from the privacy disclosures made to the data subject and the privacy protections offered and/or are outside of the jurisdiction of local privacy authorities, it may be difficult to ensure adequate controls over them and their handling of personal information.

The European approach to this challenge is to restrict all transfers of all types of personal information outside of Europe, identifying a select number of non-European jurisdictions as providing "adequate" privacy protections (Canada, Argentina, Guernsey, the Isle of Man, Israel, Switzerland, and Uruguay). These jurisdictions are deemed adequate because they have privacy laws with substantially similar requirements to the European law. This legislative choice may be partly responsible for influencing a number of countries outside of Europe to adopt privacy laws based on the European model and more likely to be deemed "adequate" in the future. Any transfers outside of Europe or the adequate jurisdictions requires execution of model contractual clauses, prescribed by law and not subject to negotiation or modification or satisfaction of a few other limited statutory bases. The only tailored content is the name of the contracting entities, a description of the types of personal information being transferred and purposes for the transfer. Transfers to unaffiliated third parties within Europe must be accompanied by the execution of certain privacy and security terms to ensure that personal information is processed according to law and the privacy notice provided to the particular data subjects.

In the United States, there is no restriction on cross-border transfers, but transfers of regulated personal information to third parties may require certain contractual privacy and security terms, such as under HIPAA for Business Associates. The U.S. state of Massachusetts, for example, also requires data security provisions to flow down through contract to all service providers with access to the personal information of Massachusetts residents (defined narrowly as a resident's name along with a social security number, driver's license number or financial account number with any necessary access codes). In addition, many U.S. states impose data breach notification obligations not only on the primary data collector but also on those entities that may store or process the data on behalf of such covered entities. These laws reflect a preference for imposing data security obligations more broadly than data privacy obligations.

Other countries that restrict third-party and cross-border transfers specifically, like Europe, simply require some contractual vehicle for ensuring that adequate data protections flow down to all entities who may have access to the covered data but do not prescribe the precise contractual language.

Policymakers considering implementation of third-party and cross-border transfer restrictions should consider:

- Any effect such restrictions may have on new market entrants, especially start-ups or smaller companies that may not be able to establish a local presence and could derive efficiencies from processing the data remotely or through sub-contractors
- What are the least restrictive means available for ensuring that all parties with access to personal information of residents are bound by the privacy promises made at the time of collection? Sometimes extending liability for the acts of all sub-contractors and agents on the primary collector can accomplish this goal
- What effect could such restrictions have on other sectors outside of mHealth (e.g., outsourcing sector, technology start-ups, cloud storage providers, etc.)

ENFORCEMENT AND SANCTIONS

Covered entities must be held accountable for complying with data privacy and security regulations, and remedies must exist to address security breaches and privacy violations. Current legislation takes vastly different approaches to this principle. Some provide for administrative fines only (and some are quite modest), while others provide for substantial fines and civil penalties. Punitive and exemplary damages are available in some jurisdictions where bad faith or willfulness can be demonstrated. Some regulatory authorities also retain the ability to impose sanctions on covered entities, imposing regular third-party audits and enhanced reporting requirements.

Along with the consideration of what levels of fines and sanctions to impose, policymakers should also consider what enforcement resources are available to carry out and enforce the laws and ensure that violations are timely punished. A number of countries with privacy laws are still rarely enforcing them, which sends the wrong message to covered entities and to the citizens that the laws aim to protect.

CONCLUSION

In addition to the areas of further study noted above, the mHealth community should also consider what mechanisms to employ to promote enforcement and compliance with mHealth privacy and security standards (legal and beyond), including developing awareness training models and training and certification approaches for providers and other data recipients. This paper only begins to lay a foundation for further research and discussion to create viable privacy and data security solutions that continue to encourage the growth and success of mHealth.

PARTNERS

The mHealth Alliance serves as an impartial, collaborative advocate for using mobile technologies to improve health around the world, with a focus on low- and middle-income countries. The Alliance is building a coalition of organizations across all sectors to openly exchange knowledge and drive collective action to mainstream mHealth, based on a shared belief that greater integration of mobile technologies will have a positive impact on key health issues globally. Hosted by the United Nations Foundation, the mHealth Alliance's founding partners include Rockefeller Foundation, Vodafone Foundation, the GSM Association and Norad. It also hosts Health Unbound (HUB), a global online community, and serves as secretariat to two innovative partnerships, the Mobile Alliance for Maternal Action (MAMA) and mPowering Frontline Health Workers. For more information, visit http://www.mHealthAlliance.org.

Founded in 1949, Baker & McKenzie advises many of the world's most dynamic and successful business organizations through more than 4,000 locally qualified lawyers and 6,000 professional staff in 72 offices in 45 countries. The Firm is known for its global perspective, deep understanding of the local language and culture of business, uncompromising commitment to excellence, and world-class fluency in its client service. Eduardo Leite is Chairman of the Executive Committee. (www.bakermckenzie.com)

Today's Merck is a global healthcare leader working to help the world be well. Merck is known as MSD outside the United States and Canada. Through our prescription medicines, vaccines, biologic therapies, and consumer care and

animal health products, we work with customers and operate in more than 140 countries to deliver innovative health solutions. We also demonstrate our commitment to increasing access to healthcare through far-reaching policies, programs and partnerships. For more information, visit www.merck.com and connect with us on Twitter, Facebook and YouTube.

Since 1965 Doulah & Doulah
ADVOCATES, ATTORNEYS & NOTARIES

D&D is a leading law firm in Bangladesh with top-ranked transactional capabilities complemented by a strong litigation practice. With twenty-nine lawyers it represents world's largest businesses in Bangladesh. Partner details are available at **www.doulah.net**.

MASEMBE, MAKUBUYA, ADRIKO, KARUGABA & SSEKATAWA ADVOCATES (MMAKS ADVOCATES)

ALN

MMAKS Advocates is a full service law firm, focused on banking, corporate and commercial law, acquisitions and intellectual property, mining and energy among others, as well as litigation in the related areas. The firm also takes a keen interest in pro bono work and corporate social responsibility.

Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

Nishith Desai Associates (NDA) is a research based international law firm with offices in Mumbai – Nariman Point, Bangalore, Silicon Valley, Singapore, New Delhi and Mumbai – Bandra Kurla Complex. We specialize in strategic legal, regulatory and tax advice coupled with industry expertise in an integrated manner. We focus on niche areas in which we provide significant value and are invariably involved in select highly complex, innovative transactions. Our key clients include marquee repeat Fortune 500 clientele.

Core practice areas include International Tax, International Tax Litigation, Litigation & Dispute Resolution, Fund Formation, Fund Investments, Capital Markets, Employment and HR, Intellectual Property, Corporate & Securities Law, Competition Law, Mergers & Acquisitions, JVs & Restructuring, General Commercial Law and Succession and Estate Planning. Our specialized industry niches include financial services, IT and telecom, education, pharma and life sciences, media and entertainment, real estate and infrastructure.

TEMPLARS

Templars is one of the leading full service commercial law firms in Nigeria, providing innovative commercial solutions for clients with diverse needs. Its specialized practice groups and expert lawyers make it a one-stop shop for bespoke legal services.

FRONT COVER PHOTO A woman uses her mobile phone with her baby in Manila. REUTERS/Cheryl Ravelo

THOMSON REUTERS
FOUNDATION

Thomson Reuters Foundation
30 South Colonnade
London E14 5EP
United Kingdom