SPECIAL REPORT

2018 DIGITAL HEALTH YEAR IN REVIEW:

FOCUS ON CARE COORDINATION AND REIMBURSEMENT

FEBRUARY 5, 2019

McDermott Will & Emery

McDermott Will & Emery

SPECIAL REPORT

TABLE OF CONTENTS

LEARN MORE

For more information, please contact your regular McDermott lawyer, or:

JAMES A. CANNATTI III
PARTNER
jcannatti@mwe.com
Tel +1 202 756 8866

DANA DOMBEY
PARTNER
ddombey@mwe.com
Tel +1 305 329 4453

AMANDA ENYEART
PARTNER
aenyeart@mwe.com
Tel +1 312 984 5488

LISA SCHMITZ MAZUR
PARTNER
lmazur@mwe.com
Tel +1 312 984 3275

DALE C. VAN DEMARK
PARTNER
dcvandemark@mwe.com
Tel +1 202 756 8177

For more information about McDermott Will & Emery visit mwe.com

INTRODUCTION

In 2018, even more than in recent years, federal lawmakers and regulators continued the push toward modernizing the existing legal framework to support and encourage digital health adoption in the context of care coordination and the move to value-based payment. These efforts brought changes to coverage of telehealth and other virtual care services, as well as information gathering for regulatory reform.

McDermott is pleased to bring you this review of key developments that shaped digital health in 2018, along with planning considerations and predictions for the digital health frontier in the year ahead.

REGULATORY SPRINT TO COORDINATED CARE

In 2018, the US Department of Health and Human Services (HHS) launched the Regulatory Sprint to Coordinated Care, which, as described by the Centers for Medicare & Medicaid Services (CMS), is focused on "identifying regulatory requirements or prohibitions that may act as barriers to coordinated care, assessing whether those regulatory provisions are unnecessary obstacles to coordinated care, and issuing guidance or revising regulations to address such obstacles and, as appropriate, encouraging and incentivizing coordinated care."

As we reported in 2018, as part of the initiative, CMS issued a broad request for information (RFI) related to potential changes in the federal physician self-referral law (Stark Law) with a goal of "reducing regulatory burden and dismantling barriers to value-based care transformation, while also protecting the integrity of the Medicare program." Similarly, the HHS Office of Inspector General (OIG) issued an RFI on how to address regulatory provisions in the anti-kickback statute (AKS) and civil monetary penalties (CMP) law that may hamper coordinated care or value-based care, as well as information on novel financial arrangements implicated by the AKS (click here for our analysis).

The HHS Office for Civil Rights (OCR) also issued an RFI to solicit comments and feedback from stakeholders on whether the HIPAA Rules should be modified to better facilitate the health care industry's transformation to value-based health care and the coordination of care. We cover the OCR RFI in more detail in Digital Health Year in Review: Focus on Data.

Value-based payment models and the digital health tools on which they may rely often implicate all three laws—Stark, AKS and CMP. The RFIs were critical opportunities to address the need for clear pathways for leveraging digital health technologies to facilitate the development and implementation of alternative service and payment models, as well as the promotion of care coordination.

The Stark RFI particularly focused on the identification of Stark Law elements that create a potential barrier to coordinated care structures. A common strategy that larger health systems and other providers use to build coordinated care models is subsidizing the use of costly tools related to electronic health records (EHR), cybersecurity

technologies and telehealth offerings by other providers. A number of the submitted comments noted that subsidization arrangements may be implicated by the Stark Law and that clearer protections should be added for such arrangements.

The AKS/CMP RFI, among other requests, solicited information regarding the donation or subsidization of cybersecurity-related items and services, perhaps in response to the Stark RFI comments. These arrangements typically are similar in design and purpose to the subsidization of EHR systems for providers by large health systems or other structures. Similar to the Stark RFI responses, a number of comments in response to the AKS/CMP RFI encouraged protections for the subsidization of infrastructure, including EHR technology, telehealth and cybersecurity resources.

The AKS/CMP RFI also sought comments on how to clarify a new exception to the definition of "remuneration" in the beneficiary inducement provisions of the CMP law enacted in Section 50302(c) of the Bipartisan Budget Act of 2018 (BBA). The exception applies to "telehealth technologies" provided on or after January 1, 2019, by a provider to individuals with end-stage renal disease (ESRD) receiving home dialysis. However, the act fails to define "telehealth technologies," stating only that the term would be defined by the Secretary of HHS. The AKS RFI sought input on how "telehealth technologies," as used in CMP law exception, should be defined, and whether "telehealth technologies" should be expanded to include telehealth services. The OIG further questioned whether any additional protections or safeguards should be implemented for the exception. Submitted commentary regarding telehealth technologies urged that the definition be expanded to include not only the technology itself, but devices required for data transmission and services related to installing the technology.

CHANGES TO PAYMENT LAWS AND RULES

As reported in detail in our Digital Health Mid-Year Report: Focus on Medicare, 2018 opened with the expansion of Medicare coverage for certain telehealth and virtual services. This expansion permitted providers to bill separately for remote patient monitoring (RPM) services conducted in connection with chronic care management, transition care management and general behavioral health integration, and included additional telehealth services codes covering health risk assessments, psychotherapy, chronic care management and interactive complexity. This expansion was quickly followed by the enactment of the BBA on February 9, 2018, which set the stage for a wide-ranging expansion of telehealth and ended with a series of proposed and final rules aimed at implementing those expansions. In addition, CMS continued its evolutionary expansion of virtual and telehealth services.

EXPANSION OF MEDICARE COVERAGE FOR TELEHEALTH SERVICES

Telehealth Stroke, ESRD and Other Services

On November 1, 2018, CMS issued a final rule updating the Medicare Physician Fee Schedule (PFS Final Rule) to implement recent telehealth-related legislative reforms enacted by the BBA. Beginning in 2019, patients presenting with stroke symptoms at hospitals or mobile stroke units may receive a timely telehealth consultation with a neurologist in order to determine the best course of treatment. In addition, patients with ESRD who receive home dialysis may choose to receive certain monthly ESRD-related clinical assessments via telehealth, provided that at least one visit in the first three months of home dialysis, and one visit every three months thereafter,

occurs via an in-person face-to-face visit without the use of telehealth. Both the home of an individual with ESRD and an ESRD facility qualify as an originating site with respect to the monthly clinical assessments (but no facility fee will be paid when the originating site is a patient's home).

Both the telehealth stroke and ESRD assessment provisions eliminate the current geographic restriction that limits originating sites to rural areas, meaning distant site providers delivering telestroke and ESRD assessment services could receive a professional fee for delivering the consultation to patients located anywhere in the United States, provided that the other Medicare telehealth coverage requirements are satisfied (*e.g.*, type of provider, type of technology).

CMS also finalized changes to the list of telehealth services eligible for reimbursement to include codes related to certain prolonged preventive services.

2018 opened with the expansion of Medicare coverage for certain telehealth and virtual services. This expansion permitted providers to bill separately for remote patient monitoring (RPM) services conducted in connection with chronic care management, transition care management and general behavioral health integration, and included additional telehealth services codes covering health risk assessments, psychotherapy, chronic care management and interactive complexity.

Expansion of Telehealth Services for the Treatment of Substance Use Disorders

In October 2018, Congress passed the Substance Use Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities (SUPPORT Act) to address the US-wide opioid epidemic. The SUPPORT Act, which we discuss on our *Of Digital Interest* blog, expands the use and coverage of telehealth services by eliminating certain requirements for substance-use disorder services under Medicare, such as geographic restrictions for telehealth. After July 1, 2019, Medicare beneficiaries may receive coverage for telehealth services related to substance-use disorders in any location, including their homes, regardless of whether the location is in a geographic area experiencing provider shortages. The PFS Final Rule includes an interim final rule with comment period that implements the new originating sites and removal of geographic restrictions.

The SUPPORT Act also directs CMS to issue (1) guidance to states regarding reimbursement for substance-use disorder treatment services, including assessment, medication-assisted treatment, counseling and medication management, using services delivered via telehealth, and (2) a report to Congress identifying best practices and potential solutions to barriers related to the delivery of services to children via telehealth. In addition, the SUPPORT Act permits incentive payments to behavioral health

providers for adoption of certified EHR technology, and includes the Special Registration for Telemedicine Act of 2018, which requires the Attorney General to promulgate, prior to October 2019, final regulations specifying circumstances in which certain providers may be issued special registrations to prescribe controlled substances via telehealth.

Opportunities for Accountable Care Organizations

On August 9, 2018, as part of CMS's "Pathways to Success" overhaul of Medicare's Accountable Care Organization (ACO) program, CMS released a proposed rule to implement changes mandated by the BBA and allow certain ACOs (*i.e.*, those participating in performance-based risk under the prospective assignment method) the opportunity to expand telehealth services by removing various barriers to the provision of telehealth services. If adopted as proposed, the revisions would, beginning in 2020, allow certain ACOs to offer their assigned beneficiaries designated telehealth services in the patient's home and eliminate the geographic component of the originating site requirement, permitting beneficiaries of eligible ACOs in urban areas to receive Medicare-covered telehealth services. Medicare reimbursement for the services would be contingent upon the telehealth services being delivered to a beneficiary at an appropriate approved originating site, such as a hospital or the beneficiary's place of residence. The provision would not retain the separate payment for the originating site fee if the service is furnished in the patient's home. Comments to the Pathways to Success proposed rule were due on October 16, 2018.

Opportunities for Medicare Advantage Plans: Telehealth Services for Chronically Ill

As we reported last year, on October 26, 2018, CMS released a proposed rule that would permit Medicare Advantage (MA) plans to provide medical care via telehealth technologies consistent with the BBA. If finalized as drafted, the telehealth regulations set forth in the MA proposed rule would affect a broad range of providers and health care companies involved in the provision or delivery of telehealth services. MA plans would be able to include in their basic benefit packages any health benefit covered by Medicare Part B that the plan identifies as "clinically appropriate" to be furnished electronically by a remote physician or other practitioner, as described in the plan's Evidence of Coverage document. In a press release announcing the MA proposed rule, CMS noted that the "additional telehealth benefits in MA will increase access to patient-centered care by giving enrollees more control to determine when, where, and how they access benefits." CMS accepted comments on the proposed rule through December 31, 2018.

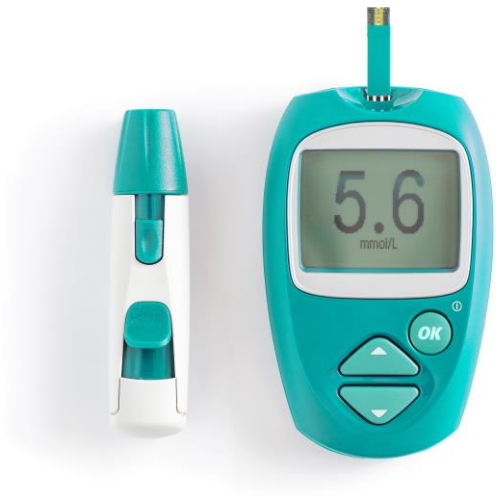
PAYMENT FOR OTHER TECHNOLOGY-BASED SERVICES

In addition to the revisions implementing BBA telehealth policy, the PFS Final Rule also finalized CMS's proposal to recognize and provide payment for a discrete set of services that are "defined by and inherently involve the use of communication technology." As described in our Digital Health Mid-Year Report with respect to then-proposed additions, these services include brief virtual visits by qualified providers to existing patients, review of patient images or videos, and certain provider-to-provider consultations. In establishing payment for these services, CMS acknowledges that recent innovations in health care have given rise to the development of services that inherently require the

use of communication technology but do not necessarily fit into the telemedicine category. CMS also finalized policies to pay separately for new coding describing chronic care remote physiologic monitoring.

REMOTE PATIENT MONITORING IN HOME HEALTH

On November 13, 2018, CMS issued a final rule to permit, as of July 1, 2019, the cost of RPM as an allowable operating cost on the cost report of a home health agency (HHA), and the allocation of the costs to the HHA's cost per visit. The regulation defines RPM as "the collection of physiologic data (for example, ECG, blood pressure, glucose monitoring) digitally stored and/or transmitted by the patient or caregiver or both to the home health agency." In announcing the revisions on its website, CMS recognized that studies have found that RPM "has a positive impact on patients as it allows patients to share more live-time data with their providers and caregivers, which will lead to more tailored care and better health outcomes." CMS noted that this change could encourage more HHAs to adopt the technology.



DIGITAL HEALTH OVERSIGHT AND ENFORCEMENT ACTIVITIES

In 2018 enforcement agencies continued to focus on digital health, highlighting the need for digital health companies to continue to strengthen corporate compliance, risk management and quality assurance programs to proactively identify and respond to issues.

TELEHEALTH PAYMENTS

In April 2018, OIG issued a report containing findings from its audit of Medicare payments for telehealth services. OIG had previously announced its plan to review telehealth service claims where there was no corresponding claim submitted by the originating site, indicating that the originating site might not have met Medicare's telehealth coverage requirements. OIG found that of the 100 claims it reviewed in its sample, 31 did not meet Medicare requirements. OIG estimated that over the two-year period covered by its audit, Medicare paid approximately $3.7 million for unallowable telehealth service claims. The focus on telehealth payments continues—according to its Work Plan, OIG is still reviewing Medicaid telehealth service payments. Effective compliance programs can help telehealth companies reduce the risk of negative findings should they find themselves on the other end of a government audit.

CYBERSECURITY OF NETWORKED MEDICAL DEVICES

In late 2018, OIG issued two reports that, although focused on the US Food and Drug Administration (FDA), could have a significant impact on the digital health industry depending on how FDA responds. The first of these reports evaluated how

FDA reviewed cybersecurity for networked medical devices in connection with premarket submissions. The second examined the effectiveness of FDA's plans for responding to a device compromise in the postmarket context. OIG concluded in both reports that the FDA could do better and made recommendations for improvements.

Whether in response to OIG's oversight or of its own accord, FDA was active in the cybersecurity space in late 2018, issuing a draft guidance document concerning cybersecurity and premarket submissions, as well as entering into relationships—within government and with the industry—to share threat and vulnerability information. OIG and FDA's increased focus on the cybersecurity of networked devices likely will affect how manufacturers, purchasers and users approach medical device cybersecurity moving forward.

DOJ ENFORCEMENT – TELEMEDICINE AND COMPOUNDED MEDICATION

There was a flurry of activity from the US Department of Justice (DOJ) in 2018 in connection with an alleged nationwide telemedicine scheme that, according to the government, involved doctors prescribing unnecessary compounded medications for patients with whom they did not have an actual doctor/patient relationship or to whom they did not provide patient care.

One telemedicine company and its owner pleaded guilty for their roles, others were charged, and some were convicted and sentenced. In a recently filed criminal complaint, the federal government referenced, but did not identify, five specific telemedicine companies involved in a similar scheme. We may see more enforcement activity surrounding telemedicine and compounded medications in 2019.

OIG'S APPROVAL OF TELEMEDICINE DONATION ARRANGEMENT

In 2018, OIG opined favorably on a proposed donation arrangement involving telemedicine items and services that was intended to facilitate HIV-prevention-related telemedicine encounters. Under the proposal, a nonprofit federally qualified health center look-alike would use state grant funds to provide certain telemedicine items (*e.g.*, a computer, microphone and camera) and services (*e.g.*, communication links/connectivity, training, maintenance and technical assistance) to a clinic operated by a county department of health approximately 80 miles away. In explaining why it concluded that the proposed arrangement would present a low risk of fraud and abuse, OIG highlighted safeguards that were designed to prevent inappropriate patient steering, the fact that the arrangement would be unlikely to result in inappropriate increases in federal health care program costs, and the fact that the clinic patients were the ones who would primarily benefit from the arrangement. Such factors are constant with those addressed in OIG's previous reviews of telemedicine arrangements.

OIG found that of the 100 claims it reviewed in its sample, 31 did not meet Medicare requirements. OIG estimated that over the two-year period covered by its audit, **Medicare paid approximately $3.7 million for unallowable telehealth service claims.**

OIG ISSUES STIPULATED PENALTIES FOR EHR-RELATED CORPORATE INTEGRITY AGREEMENT

In July 2018, OIG announced that eClinicalWorks, LLC (eCW) had paid more than $130,000 in stipulated penalties for its failure to comply with corporate integrity agreement (CIA) reporting obligations related to patient safety issues. As we reported here, eCW had entered into the novel CIA in 2017 as part of a DOJ settlement over allegations that eCW had caused its customers to submit false claims for Medicare and Medicaid EHR incentive payments in violation of the False Claims Act. The stipulated penalties demonstrate that OIG takes compliance with the terms of its CIAs seriously.

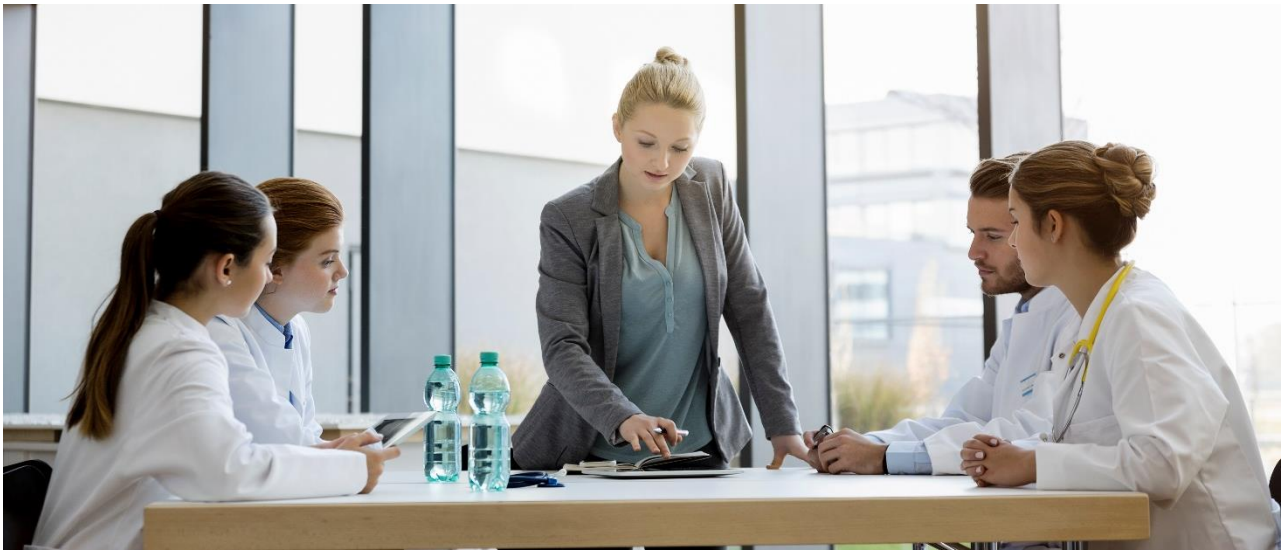
HOW SHOULD DIGITAL HEALTH COMPANIES RESPOND IN 2019? FOCUS ON USE-CASES AND INVEST IN COMPLIANCE

Over the past few years, both Congress and CMS have clearly demonstrated their willingness to improve the economic environment for digital health solutions. It is equally clear, however, that neither has an interest in simply providing reimbursement for every digital health solution that might exist. At the same time, as digital health continues its march into the mainstream, regulatory oversight and enforcement are becoming a more pressing reality. Accordingly, digital health companies and programs need to be smart about growth and expansion.

Within the third-party payor system, digital health continues to be tied directly to specific payment programs. While the universe of reimbursable activity is expanding, it is not infinite and still must be matched to what the payment program recognizes. For reimbursement purposes, digital health continues to be use-case driven. And that is what digital health companies should be focused on, in terms of both immediate applications and advocacy for expanded reimbursement.

As demonstrated by the regulatory oversight and enforcement activity in 2018, digital health companies should continue investing in the design and implementation of effective compliance programs. Effective compliance programs:

- Establish an overall framework of policies, procedures and protocols that govern the company's employees, contractors and officers



- Support a culture of integrity and accountability
- Promote the prevention, detection and correction of conduct that does not live up to the company's policies and procedures, or does not conform to applicable laws, regulations, or federal, state or private payer health care program requirements (as applicable)

Digital health companies of all shapes and sizes should develop compliance programs that are responsive to the company's specific needs, based on its size, activities, financial resources, areas of legal risk exposure and other relevant factors.

The OIG has published Compliance Program Guidance that includes seven fundamental and widely recognized elements of an effective compliance program that are aimed at accomplishing these rather lofty objectives.

Digital health companies of all shapes and sizes should develop compliance programs that are responsive to the company's specific needs, based on its size, activities, financial resources, areas of legal risk exposure and other relevant factors. Digital health companies (even those providing similar or identical types of services, such as direct-to-consumer telehealth) each will have unique policies and procedures, auditing and monitoring practices, and governance oversight structures, as they are likely focused on different areas of compliance risk and have different financial resources to invest in compliance-focused oversight activities.

A compliance program also should take into account specific emerging areas of risk based on regulatory enforcement activity and anticipated or newly enacted changes to the law. For example, based on 2018 activity, a telehealth company's compliance program should focus on the maintenance and enhancement of care quality, internal monitoring of compliance with telehealth state laws and regulations, and compliance with government payer billing and coding rules.

- To view the first issue in our 2018 Digital Health Year in Review series, *Focus on Data*, click here.
- For more information on the latest Digital Health developments, click here.

CONTRIBUTORS

JAMES A. CANNATTI III
PARTNER
jcannatti@mwe.com
Tel +1 202 756 8866

DANA DOMBEY
PARTNER
ddombey@mwe.com
Tel +1 305 329 4453

AMANDA ENYEART
PARTNER
aenyeart@mwe.com
Tel +1 312 984 5488

LISA SCHMITZ MAZUR
PARTNER
lmazur@mwe.com
Tel +1 312 984 3275

DALE C. VAN DEMARK
PARTNER
dcvandemark@mwe.com
Tel +1 202 756 8177

NICOLE B. SANDLER
ASSOCIATE
nsandler@mwe.com
Tel +1 305 329 4487

PATRICK ZANAYED
ASSOCIATE
pzanayed@mwe.com
Tel +1 312 984 2029

BOSTON
28 State Street
Boston, MA 02109-1775
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9 - 31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
444 West Lake Street
Chicago, IL 60606-0029
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DALLAS
2501 North Harwood Street
Suite 1900
Dallas, TX 75201-1664
USA
Tel: +1 214 295 8000
Fax: +1 972 232 3098

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
Tel: +49 69 951145 0
Fax: +49 69 271599 633

HOUSTON
Two Allen Center
1200 Smith Street
Suite 1600
Houston, TX 77002-4403
USA
Tel: +1 713 653 1700
Fax: +1 972 232 3098

LONDON
110 Bishopsgate
London
EC2N 4AY
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East
38th Floor
Los Angeles, CA 90067-3218
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 SE 2nd Avenue
Suite 4500
Miami, FL 33131-2184
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via Dante 15
20123 Milan
Italy
Tel: +39 02 36575701
Fax: +39 02 36575757

MUNICH
Nymphenburger Str. 3
80335 Munich
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173-1922
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
18565 Jamboree Road
Suite 250
Irvine, CA 92612-2532
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

SAN FRANCISCO
415 Mission Street
Suite 5600
San Francisco, CA 94105-2533
USA
Tel: +1 628 218 3800
Fax: +1 628 218 3900

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 04539
Korea
Tel: +82 2 6030 3600
Fax: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R.China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road
Suite 100
Menlo Park, CA 94025-4004
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, DC
The McDermott Building
500 North Capitol Street, NW
Washington, DC 20001-1531
USA
Tel: +1 202 756 8000
Fax: +1 202 756 808

McDermott
Will & Emery

mwe.com |