McDermott Will & Emery

ISSUE 2 2017

IN

International News

FOCUS ON

Health Care

Enforcing a Commercial US Arbitration Award in India

New European Personal Data Breach Obligations on the Horizon

Spotlight on China's Hospital System

EDITOR
Andrea Hamilton
Partner
Brussels
+32 2 282 35 15
ahamilton@mwe.com

PUBLICATION EDITORS
Aileen Devlin
Kate Hinze

CREATIVE SERVICES
Christine Abrego
Valerie Green

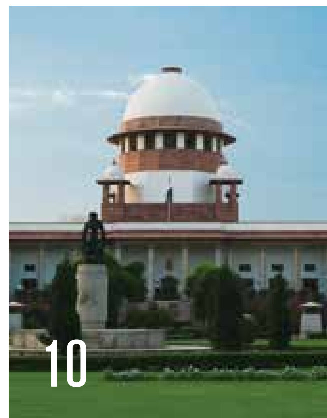
Health care systems across the world are facing similar challenges, regardless of their regulatory or cultural differences. From this however, lessons can be learned in one jurisdiction and applied elsewhere: the US accountable care organisations model has come to the UK as accountable care systems; and the proliferation of cross-border joint ventures and affiliations between governments and health care providers and operators generate templates for what works and what doesn't.

In the same vein, the United States is increasingly adopting European loyalty share programmes, and the EU General Data Protection Regulation (GDPR) comes into effect next year. The GDPR will harmonise data protection across Europe for the first time, and affect any business, regardless of location, that has a connection with EU-originating personal data.

Shared experiences and common purpose vary in other areas. Globalisation is out and nationalism in, as recent aborted deals demonstrate. Nationalism appears to be more prevalent in developed countries and may actually prove to be an advantage for emerging markets that want to play a larger role on the global stage.

Please contact me if you have any comments on our articles or would like to discuss any of the issues raised.

TABLE OF CONTENTS



FEATURES

3 Nationalism and Cross-Border M&A: Navigating populist politics in deal making
David Dai and Jacob A. Kuipers

6 New European Personal Data Breach Obligations on the Horizon
Mike Morgan, Paul McGrath and Antonina Nijran

8 Rewarding Long-Term Shareholders: European and US Loyalty Share Programmes
Thomas Conaghan, Lionel Lesur, Lindsey Reighard and Louis Leroy

10 Enforcing a Commercial US Arbitration Award in India
Daniel Foster and Jodi Benassi

FOCUS ON > HEALTH CARE

11 Going Global – International Health Care Joint Ventures and Affiliations
Hamid Yunis

14 Artificial Intelligence in Health Care: Framework Needed
Dale Van Demark

16 Spotlight on China's Hospital System
David Dai and Jenny Wang

18 Accountable Care in the United Kingdom: Learning From International Experience
Sharon Lamb

Nationalism and Cross-Border M&A: Navigating Populist Politics in Deal Making

DAVID DAI AND JACOB A. KUIPERS

More than half of the G20 countries voted-in campaigns that focused on harming foreign, outside interests as a means to strengthen domestic ones. Nationalism is in. Globalisation is out.

CONTINUED >

Nationalistic rhetoric is proliferating across the global political landscape. From India, and Prime Minister Narendra Modi's "India First," to the United States, and President Donald Trump's "Make America Great Again," politicians are scoring popularity points and galvanising voters who yearn for national glory.

With increased nationalism, two elements of globalisation—the free flow of goods and services (trade) and people (immigration)—have come under attack across the world, where protectionist and anti-immigration policies are disrupting the globalised world order. The third element—the free movement of money or investment—also might not be immune to nationalism.

Several anecdotes signify that a rise in nationalism could jeopardise cross-border investments and deals. Two of the most recent include Ant Financial's (China) takeover of MoneyGram (US), and the implosion of PPG Industries' (US) prolonged pursuit of Akzo Nobel (Netherlands). These examples do not necessarily mean that increased nationalism translates into a decline in international deal-making. Nevertheless, nationalism is a risk variable that further adds to the complexity and prickly nature of cross-border investment and M&A.

ANT FINANCIAL AND MONEYGRAM DEAL IN LIMBO

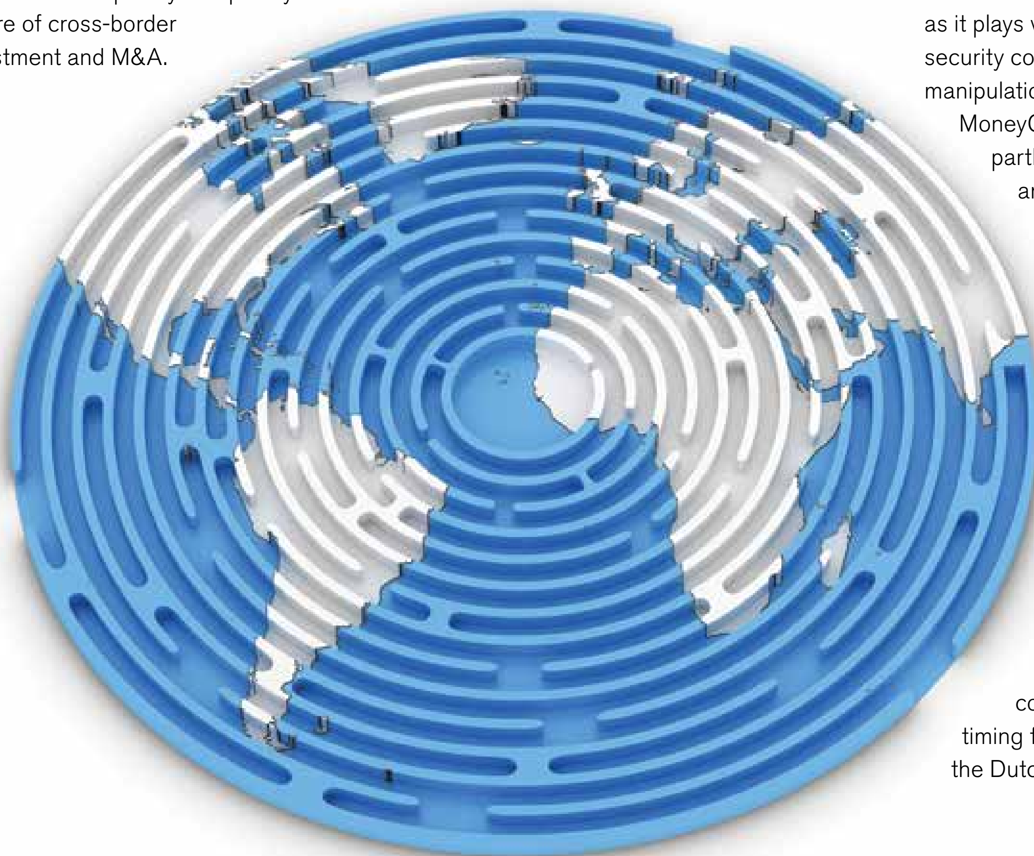
Since January 2017, Ant Financial, which is headquartered in China and is the financial payments affiliate of Chinese e-commerce giant Alibaba, has been battling Euronet, a US-based financial payment provider, to acquire MoneyGram, a US-based cross-border payments service. After much negotiation among the three companies, Ant Financial prevailed over Euronet with a US$1.2 billion offer in April 2017.

> "International deal making is not necessarily doomed."

Throughout the negotiations, and even since MoneyGram accepted Ant Financial's offer, Euronet stressed security and data privacy concerns over having a Chinese company control a US-based payments provider. Euronet has repeatedly pushed the idea that because Ant Financial is owned primarily by Chinese investors, it does not meet sufficient standards for being a US money transmitter.

Someone in the US Government may have been listening to Euronet. On 11 July 2017, Ant Financial was forced to resubmit the deal for review by the Committee on Foreign Investment in the United States (CFIUS) after failing to obtain clearance within the normally allotted 75 days. CFIUS performs a national security review of all acquisitions of US companies by foreign entities. The fact that Ant Financial could not obtain clearance within the normal review period reflects a heightened level of scrutiny by the US Government. US Senator Jerry Moran, who represents the state where Euronet is headquartered, has spoken publicly and advocated to CFIUS that the deal represents a significant security concern to US citizens.

Against the political backdrop of President Trump's America First foreign policy agenda, the commercial relationships between US and Chinese companies are complex and difficult to gauge. Nevertheless, Euronet's security concern claim places its and the Trump Administration's interests in alignment, as it plays well with the Administration's security concern over Chinese financial manipulation. The Ant Financial–MoneyGram deal remains in limbo, partly owing to nationalist rhetoric and policy, putting MoneyGram's shareholders at risk of taking Euronet's smaller (by US$200 million) bid if CFIUS rejects Ant Financial's deal.



PPG GIVES UP ON AKZO NOBEL

In early March 2017, PPG Industries, a US-based paint and specialty coating manufacturer and supplier, made a US$28 billion offer to buy Dutch competitor Akzo Nobel. The timing for PPG was not good, as the Dutch national elections, which

were largely dominated by anti-foreign, pro-national rhetoric, were to occur a few weeks later. The Dutch public had grown increasingly concerned over foreign acquisitions of Dutch companies. This concern was further stoked by nationalist leaning politicians who attempted to tie foreign acquisitions to a loss in Dutch identity.

Even after the elections, in which more moderate politicians prevailed, Dutch politicians continued to oppose the deal, culminating with multiple provinces, as well as the Dutch Economic Affairs Minister, openly criticising the potential deal. They cited concerns over Dutch workers, labour standards, and the need to maintain Dutch-controlled entities.

> “Companies can use a country’s nationalist fervour to strengthen their defensive position.”

Akzo Nobel, which refused to engage in negotiations with PPG, used the nationalist political landscape to continually rebuff PPG’s advances, despite PPG making three additional offers that topped out at US$29.5 billion in May 2017. Although most Akzo Nobel shareholders approved of its defensive posture, Elliot Advisors, a hedge fund with significant holdings in Azko Nobel, attempted to get a Dutch court to remove Akzo Nobel’s management for failing to engage with PPG.

The Dutch court rejected Elliot Advisors’ arguments, finding that Akzo Nobel’s actions aligned with most shareholders’ wishes. The case, however, further strengthened the nationalist message and sent lawmakers scurrying to put in place laws that would make it harder for a foreign entity to acquire a Dutch company. On 1 June, PPG formally withdrew its offers, realising it did not have the legal or political capital to leverage the deal.

PPG’s attempt to acquire Akzo Nobel provides an example for how nationalist winds can put further pressure and embolden defensive measures against an unsolicited, foreign takeover. Without the strong political pressure in favour of Akzo Nobel’s independence, the company might have found it much harder to make its case to shareholders.

NATIONALISM ADDS FURTHER COMPLEXITY TO CROSS-BORDER M&A

Like trade and immigration, international investment and cross-border M&A are not immune to the growing wave of nationalism. The Ant Financial–MoneyGram deal shows how nationalist tendencies have the possibility of shaving US$ hundreds of millions from a company’s valuation. And PPG’s efforts to acquire Akzo Nobel reflect how companies can use a country’s nationalist fervour to strengthen their defensive position.

Although these examples suggest a negative outlook for cross-border M&A in a world of national interests, international deal making is not necessarily doomed.

First, nationalism remains strongest in large, developed economies, while cross-border M&A is growing fastest in emerging markets. Moreover, investment flows between developing countries continue to increase. For example, despite the recent setbacks in China’s high-profit acquisition projects in the United States and Europe, which is mainly attributable to rising nationalism, China’s investment in developing countries in the Middle East and South Asia under China’s One Belt One Road initiative continues to grow. As a result, international deal-making no longer relies on the mature markets where nationalism poses the greatest risk.

Second, nationalist policies like trade protectionism and anti-immigration reform do not necessarily restrict cross-border deal flow. In fact, the opposite may be true as a World Bank study found that when trade protectionism increases, international M&A and investment also increase.

Third, outbound cross-border M&A might be a mechanism for advancing a nationalist agenda. For a country that wants to play a larger role on the global stage and increase its national stature, having its domestic companies become more prominent internationally through cross-border acquisitions could be complementary. This is clearly one of the reasons behind the recent boom in China’s outbound investment.

Regardless of nationalism’s impact on international deal flow, the growth in nationalist tendencies has become a significant variable that must be addressed by any entity engaging cross borders.

Junda (David) Dai
Partner, MWE China Law
Shanghai
ddai@mwechinalaw.com

David represents a variety of European and US clients in their direct investments in China, including green-field investments, cross-border mergers and acquisitions, venture capital and private equity investments, and strategic alliances.

Jacob Kuipers
Associate
Boston
jkuipers@mwe.com

Jacob advises public and private companies on complex domestic and cross-border corporate transactions, including mergers and acquisitions, international reorganisations, and venture financings.

New European Personal Data Breach Obligations on the Horizon

MIKE MORGAN, PAUL MCGRATH AND ANTONINA NIJRAN

The EU General Data Protection Regulation (GDPR) will introduce mandatory personal data breach notification obligations across all sectors, in all EU countries, for the first time.

The GDPR will come into effect from 25 May 2018. Its extraterritorial reach means that the new data breach notification obligations will apply to any organisation located anywhere in the world that processes personal data in relation to the offering of goods or services in the European Union, or is involved in monitoring the behaviour of data subjects within the European Union. This will be the case regardless of whether or not the organisation has any physical presence or formal establishment in the European Union.

The stakes for compliance with the notification obligations are high, as failures can lead to fines of up to €10 million or 2 per cent of a company's worldwide annual turnover for the preceding financial year, whichever is higher. Individual data subjects will also have the right to bring legal claims against controllers that fail to comply.

It is therefore important for all organisations to understand the extent to which (and when) data breach notification obligations will arise under the GDPR.

HAS A PERSONAL DATA BREACH OCCURRED?

The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". In practice, this threshold is likely to be met in most cases, including instances where data is encrypted or deleted in a ransomware attack and where data is exfiltrated as part of a hack.

WHAT NOTIFICATION OBLIGATIONS ARISE IN A PERSONAL DATA BREACH?

The extent of an organisation's notification obligations in the event of a personal data breach will depend on whether, in the particular circumstances, the organisation is acting as a data controller, *i.e.*, determining the purpose and means of the data processing, or a data processor, *i.e.*, processing data on behalf and at the direction of a data controller.

Data Controller Notification Obligations

For data controllers, the default position is that personal data breaches must be reported to the relevant supervisory authority by a data controller unless the breach is "*unlikely* to *result* in a risk to the rights and freedoms of natural persons" (authors' emphasis). A data controller will need to assess whether or not a breach, if not dealt with, is likely to have a detrimental effect on the individuals concerned; for example, is the breach likely to result in discrimination, loss of confidentiality, financial loss or damage to reputation?

Whether or not a risk exists will vary depending on the nature of the data involved in the breach and the nature of the breach itself. For instance, a breach resulting in the disclosure of sensitive or financial data is likely to pose a greater risk to the rights and freedoms of an individual than a disclosure of the staff telephone list. The recitals to the GDPR suggest that a relatively low threshold will apply, however, in determining whether or not there is such a risk to people. In practice, therefore, it is anticipated that notification will be required in most cases.

Where the duty to report a breach does arise, care will need to be taken to ensure that the report is made to the correct supervisory authority. Where the personal data breach concerns cross-border processing activities, notification ought to be made to the organisation's lead supervisory authority under the GDPR's "one-stop shop" mechanism. This will be the supervisory authority of the EU Member State in which the relevant controller has its sole or main establishment, *i.e.*, where the decisions about the purposes and means of the processing are taken.

Data controllers that do not have an establishment in the European Union need to appoint a representative in one of the Member States where the data subjects, whose personal data is processed, are located. The GDPR does not place separate breach notification obligations on these representatives or expressly enable them to assume the data controller's responsibilities for breach notification in the alternative.

In contrast, data controllers will only be required to report a personal data breach to data subjects where it is "*likely* to result in a *high risk* to the rights and freedoms of natural persons" (authors' emphasis).

Whilst the GDPR does not provide specific guidance on the circumstances in which

this obligation will be triggered, the text clearly suggests a higher threshold. The GDPR enables supervisory authorities to assess matters for themselves and, where appropriate, order an organisation to notify data subjects of a breach.

Notification to data subjects will not be required in the event that the data controller has "implemented appropriate technical and organisational protection measures… in particular those that render the personal data unintelligible … such as encryption" or has taken "subsequent measures which ensure that the high risk to the rights and freedoms of data subjects… is no longer likely to materialise".

Data Processor Notification Obligations

For data processors, any personal data breach will be reportable to the data controller. Data processors will not, however, be obliged to notify a supervisory authority and/or any data subject.

WHAT TIME LIMITS APPLY?

Where breach notification obligations arise under the GDPR, the time limits for reporting are potentially onerous, adding further pressure to what is often already a crisis situation.

Data Controllers

Where a data controller concludes that the personal data breach in question is a notifiable event, the relevant supervisory authority will need to be notified "without undue delay and, where feasible, not later than 72 hours" after the controller has become aware of it.

What constitutes "undue delay" is not defined in the GDPR. For larger and more complex data breaches, where it is not possible to provide full information at the same time, the GDPR advocates providing it "in phases without undue further delay". Where notification is made outside the 72 hour window, reasons for the delay will need to be provided.

Any notifications to data subjects must also be made "without undue delay", although not necessarily within 72 hours.

Data Processors

Similarly, the obligation imposed by the GDPR on data processors is to inform the data controller "without undue delay".

WHAT INFORMATION NEEDS TO BE PROVIDED IN A REQUIRED NOTIFICATION?

Data Controllers

A report must contain the following information:

- The nature of the personal data breach.
- The name and contact details of the data protection officer (if an organisation has one) or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects of the breach.

> "It is anticipated that notification will be required in most cases."

Notifications by data controllers to data subjects require the same content, except no information about the nature of the personal data breach needs to be included. Each data subject should be notified individually, except where this would involve "a disproportionate effort". In such circumstances, communication to the affected data subjects can be carried out via "public communication or similar measure whereby the data subjects are informed in an equally effective manner".

Data Processors

There is no prescribed form which a data processor's notification to a data controller ought to take.

WHAT STEPS SHOULD ORGANISATIONS TAKE TO PREPARE?

Preparatory actions may include

- Establishing a breach response team that includes both appropriate internal staff members and relevant external advisers such as lawyers and forensic IT experts. This will aid a more rapid response in the event of a breach incident and make it easier to comply with notification obligations.
- Preparing a data breach response plan and allocating responsibilities amongst the response team.
- Developing internal data breach notification procedures.
- Training personnel to ensure prompt escalation of and responses to breach incidents.
- Running mock response exercises to identify faults and areas for improvement.
- Implementing appropriate technical security measures appropriate to the nature of the organisation's data processing activities.

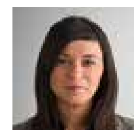
Dennis Brunner also contributed to this article.

Mike Morgan
Partner
Los Angeles/Silicon Valley
mmorgan@mwe.com

Mike is co-chair of the Firm's Global Privacy and Cybersecurity practice. He has guided clients through some of the largest and most complex data breaches, including breaches involving global data.

Paul McGrath
Partner
London
pmcgrath@mwe.com

Paul advises on privacy and data protection matters, with a particular focus on those arising in the employment context.



Antonina Nijran
Associate
London
anijran@mwe.com

Antonina advises clients across a range of industry sectors on privacy and data protection issues.

Rewarding Long-Term Shareholders: European and US Loyalty Share Programmes

THOMAS CONAGHAN, LIONEL LESUR,
LINDSEY REIGHARD AND LOUIS LEROY

Loyalty share programmes, or programmes that encourage shareholders to hold their shares for longer periods of time, have been gaining traction in Europe, but for a number of reasons they remain uncommon in the United States.

"Long-term oriented shareholders, who hold on to their shares during the difficult but critical time the company is facing [will thus be rewarded]." This is how the CEO of Michelin explained the motivation behind the issuance of loyalty shares by his company in 1991. Loyalty shares (typically in the form of additional shares or dividends) that reward shareholders who hold shares for a certain period of time, and other similar programmes, have become increasingly popular in European countries as a way to incentivise long-term shareholding.

They are now slowly making their way into the United States but there are a number of issues US companies should be aware of before launching such a programme.

EUROPEAN LOYALTY SHARE PROGRAMMES

Rewarding long-term shareholding has been subject to regulation by the European Union since 2007 when the European Parliament passed Directive 2007/36/EC to regulate the exercise of certain rights of shareholders in listed companies. The Directive provides a limited framework for encouraging a higher level of monitoring and engagement by institutional investors and asset managers, and leaves these issues in the hands of the individual EU Member States.

France offers several mechanisms to support long-term shareholding, the latest having been implemented in March 2014 with the adoption of the *Loi Florange*. French listed companies must automatically grant double voting rights to shareholders who hold their shares in registered form for at least two years, and non-listed companies may grant double voting rights to shareholders who hold their shares in registered form for the same period.

Listed and non-listed French companies may also issue L-warrants to certain shareholders, or grant loyalty dividends under certain conditions. These loyalty schemes have been implemented by many major French listed companies, such as L'Oréal, Electricité de France and Crédit Agricole (as a loyalty dividend), or Vivendi, Engie, and Air France KLM (as double voting rights).

Other European countries have adopted similar mechanisms. The Netherlands permits companies to grant multiple voting rights to certain categories of shareholders if the companies register their shares in a Loyalty Register. This scheme was notably used by Ferrari NV in its initial public offering (IPO), and by Fiat Chrysler Automobiles NV upon completion of the cross-border reverse merger by Chrysler-Fiat with and into Fiat Investments NV in 2014.

In Italy, a 2010 Legislative Decree allowed listed companies to pay increased dividends to shareholders that hold common shares for at least one year. In 2014, a reform authorised both listed and non-listed Italian companies to issue shares with multiple voting rights. These schemes have been successful, and many Italian companies, including Campari and Amplifon, have awarded loyalty shares to certain categories of shareholders.

US LOYALTY SHARE PROGRAMMES

Despite the popularity of loyalty share programmes in Europe, US companies have been slow to implement them. The US stock market is generally characterised by "short-termism": a focus on short-term results at the expense of long-term performance, driven in part by the need to report quarterly earnings. US shareholders, many of which are institutional investors, therefore tend to hold their shares for only a short period of time. According to the 2016 New York Stock Exchange (NYSE) Group turnover statistics, the annualised turnover for shares listed and traded on the NYSE at the end of 2016 was 70 per cent, indicating that a majority of shareholders held their shares for less than one year.

> "US shareholders . . . tend to hold their shares for only a short period of time."

The US Securities and Exchange Commission (SEC) attempted to promote long-term shareholding by proposing a rule that would have provided shareholders that held a significant amount of company stock for at least three years the right to include in the company's proxy statement their own director nominees. The rule was ultimately invalidated by US courts, but that did not stop companies from voluntarily, or, in response to shareholder activist demands, adopting their own proxy access bylaws.

Proxy access provisions can now be found in the bylaws of a majority of the *Fortune* 500 and, generally, they also require at least three years of ownership to be eligible to nominate director candidates for inclusion in the company's proxy statement. The SEC has, however, not yet adopted mechanisms expressly permitting loyalty shares, voting rights and dividends. Given the lack of regulatory framework, loyalty share programmes remain a novelty in the United States.

Some US companies have, however, ventured into these relatively uncharted waters. For example, The J.M. Smucker Company has adopted "time phased voting," allowing each share held for more than four years to have 10 votes per share (instead of one vote) on certain matters, and NexPoint Credit Strategies Fund has offered a 2 per cent match to shareholders who hold the fund's common shares for at least one year.

Other companies have offered warrants to purchase shares that are exercisable at a certain period of time in the future, such as Check-Cap Ltd., an Israeli company that issued warrants to its US IPO purchasers in 2015, permitting such purchasers to acquire common shares at a fixed purchase price if they held their IPO shares for a minimum of one year.

REGISTRATION OF LOYALTY SHARES

If a company decides to pursue a loyalty share programme for its US shareholders, it should consider whether or not the programme constitutes a "sale" or an "offer to sell" a security that requires registration under the Securities Act of 1933.

Depending on the facts and circumstances, the SEC might view a loyalty share as being more similar to a "right" issued in a rights offering, in that the holder can elect to exercise that right by foregoing the legal right to transfer its underlying shares, thereby accepting investment risk in exchange for receiving the loyalty share. Even though there is no exercise price for a loyalty share, there could be "value" flowing back to the company in the form of loyalty, lack of volatility and other indirect benefits that long-term shareholders provide to the company.

The SEC may also take a "remedy-based" approach, by stating that the holder who chose to "register" his "intent" to be loyal is making an investment decision. If he is "penalised" for holding the underlying shares, *i.e.*, the share price drops while he is trying to make it to the loyalty date, he should therefore be entitled to receive, as damages, the "consideration" he "paid" for registering into the loyalty share programme.

Given the novel structure of US loyalty share programmes, and the lack of precedent or specific support for loyalty shares without registration, companies would be prudent to either register such shares or, at a minimum, seek no-action relief from the SEC.

NEXT STEPS

These are only a few of the issues that a company should consider before implementing a US loyalty share programme. Because of the lack of regulatory guidance in the United States, in contrast with Europe, companies should tread carefully if they decide to proceed with such a programme in the United States.

Thomas Conaghan
Partner
Washington DC
tconaghan@mwe.com

Tom advises US- and foreign-based public companies on issues relating to corporate transactions.

Lionel Lesur
Partner
Paris and Rome
llesur@mwe.com

Lionel advises domestic and international companies on matters involving corporate and competition/distribution law.

Lindsey Reighard
Partner
Dallas
lreighard@mwe.com

Lindsey represents private and public companies in connection with US and international corporate transactions.

Louis Leroy
Associate
Paris
lleroy@mwe.com

Louis advises French and international companies on all aspects of corporate and financial law.

Enforcing a Commercial US Arbitration Award in India

DANIEL FOSTER AND JODI BENASSI

The prevailing cross-border system for dispute resolution—international arbitration—is often more predictable and less expensive than litigation. Enforcing a foreign award can, however, be arduous, especially in jurisdictions like India.

The first issue to be aware of is that there is no advantage in having a US Federal Court confirm the arbitration award and issue a judgment before seeking to enforce the award in India. An arbitral award and subsequent judgment have equal footing in the Indian judicial system insofar as recognition and execution are concerned. Once a party has the final award, it therefore may, and should, begin the enforcement process. Early engagement with Indian counsel will help effectively navigate Indian civil procedure issues.

Under the New York Convention, a US award is required to go through an enforcement procedure under which the party seeking enforcement must apply for recognition and enforcement of the award. In India these proceedings should be instituted in the relevant state or union territory High Court. The High Courts maintain jurisdiction over the enforcement of foreign awards, irrespective of the quantum of the award and they are generally adept at handling the intricacies of commercial matters.

Parties seeking to enforce awards in India should consider partnering with local counsel that possesses the right experience for the particular court and the issue at hand.

Depending on the relief being sought, award holders should consider filing the enforcement application in the High Court of the jurisdiction where the Indian company owns significant assets, rather than where the company's registered offices are located. Proper selection of the court where the enforcement proceedings will be instituted is essential to avoid needless debate on jurisdiction. Orders allowing or refusing enforcement are appealable orders under India's Arbitration Act, so the award may go from the High Court to the Appeal Court to the Supreme Court.

Public policy also plays a prominent role in the Indian judicial system, as the law mandates that only a judgment determined on the merits of the case is enforceable. Arbitral awards can be refused on grounds of public policy when the enforcement of the award would be contrary to the fundamental policy of Indian law, the interests of India, Indian justice or morality, or if the award is patently illegal under Indian law. Public policy issues are the overriding impediment to the enforcement of arbitral awards in India.

It is important that adequate notice be promptly given to the respondent Indian company of all hearings and pleadings, especially *ex parte* awards, to ensure the respondent does not have an opportunity to contend that it was not given notice nor adequate opportunity to appear and present its case before the tribunal. Without proper notice, Indian courts will likely set aside the award.

Daniel Foster
Partner
Orange County
dfoster@mwe.com

Dan litigates and tries complex intellectual property and commercial cases, and advises companies on IP licensing issues, pre-litigation strategy, licensing audits, and patent acquisition matters.

Jodi Benassi
Associate
Silicon Valley
jbenassi@mwe.com

Jodi focuses her practice on matters related to intellectual property litigation, including patents, trademarks, copyrights, and trade secrets.

Going Global – International Health Care Joint Ventures and Affiliations

HAMID YUNIS

Governments and their health care systems or operators are increasingly looking for improved, economically viable and more robust delivery of health care services. This has generated a real opportunity for entities that can provide these services to fulfil their needs.

CONTINUED >

Global health care entities, health care operators and governments are increasingly entering into cross-border joint ventures and affiliation models to gain access to best practice in an effort to better deliver health care services. Typically, the parties to such an arrangement are

> Major health care entities, such as a health care system, academic medical institution or leading hospital (referred to here for simplicity as the "international body").

> A national government, local health authority or health care operator, (referred to here as the "delivery body").

From both sides, there are a number of issues the parties should take into account when structuring a collaboration to ensure each party achieves its aims and objectives. Equally, there are a number of common pitfalls that should be avoided.

INITIAL DUE DILIGENCE

There is no substitute for being properly prepared and undertaking a thorough due diligence exercise to ascertain where the opportunities are and to mitigate any risks that may arise.

Actions that should be completed at this initial stage include the following:

> A full investigation by each party into the other's capability, validity and ability to perform.

> A thorough financial analysis that includes ensuring both parties understand, in particular, the local reimbursement policy and determining whether or not this creates a sustainable business model going forward.

> A detailed counterparty and competitor analysis to evaluate who else is active in the local jurisdiction and whether or not the joint venture or collaboration can realistically create a market leading or sustainable position.

> A comprehensive review of both parties' governance and compliance policies and an assessment of the local jurisdiction's political, financial and cultural landscape. Issues that should be considered include determining whether or not both parties have a standard of compliance with local and international anti-corruption and anti-bribery legislation.

GLOBAL AFFILIATION MODELS

The most commonly used models take the form of one of the following, or a combination or hybrid of two or more:

1. A new and independent entity set up in a local jurisdiction.
2. An outright acquisition of a business or entity, with the acquirer taking full control and governance.
3. A joint venture, which may be either a new, jointly owned entity, or an unincorporated joint venture where the partners remain independent of each other.
4. A management, services or advisory contract, that covers one or more of the following:

   a) Clinical management, on a macro or specific basis

   b) Access to data, analytics and IT

   c) Infrastructure consultancy, *i.e.*, for the development of facilities, the supply of equipment and the provision of services, *etc.*

   d) Discrete elements specific to one area of clinical delivery, *e.g.*, oncology, telemedicine or sports science, *etc.*

   e) Delivery of training, research and development services

   f) Replicating service delivery standards from the international body's home market into a foreign jurisdiction.
5. Licensing of intellectual property
6. The provision of staff.
7. Financial or other technical support.

LICENSING OF IP OR BRAND NAMES

There is another option: agreements for the use of brand names(s). This type of arrangement should, however, be avoided as it is extremely difficult to ensure real oversight and quality assurance. A failure to cover this properly could lead to substantial risks, including an adverse reputational impact and a danger of wider contamination.

ADDITIONAL ISSUES TO CONSIDER

Before coming to a final agreement, both parties should give considerable thought to the following points.

Identifying the Right Arrangement

From the point of view of the international entity, it may make sense to have a specific entity, or special purpose vehicle, within its organisational structure to hold its interest in the venture.

In addition to being preferable from a fiscal, regulatory and tax point of view, this also creates an easier and more transparent structure to provide oversight and deal with disputes if they do arise.

The international entity needs to be certain that the delivery body has the capacity and ability to enter into the chosen arrangement.

Scoping the Requirements

Each party needs to know, and be clear with the other party, what its aims and objectives are from the outset.

Marketing the Collaboration

The collaboration must be marketed properly to ensure both parties achieve their goals.

Determine Whether or not Financing is Required

Parties should determine the type of funding that is required and what, if any, future funding requirements might be needed as the arrangement progresses.

In particular, it is worth considering a time-based funding requirement and how this will impact on the economic or ownership rights of the entity that implements the arrangements.

Appointing Key Representatives and Forming a Committee

It is very helpful to have some form of management or liaison committee that includes representatives from both the international body and the delivery body.

This committee could deal with the management of the arrangements, any dispute resolution process, and what the next steps should be if the arrangement is a success or a failure.

Dispute Resolution Mechanism

It is vital to incorporate a dispute resolution procedure that allows for a sensible escalation for dispute resolution, depending on the seriousness of the dispute. For example, the local representative could report to a more senior representative, and ultimately to a CEO level person. If that fails, there could be recourse to arbitration or, ultimately, to court proceedings.

> “It is vital to incorporate a dispute resolution procedure.”

Human Resources

One of the main reasons for the failure of these types of collaboration is a scarcity of, or lack of agreement on, human resources. These may include transfers of staff or the parties' differing views on who is a "fit and proper" person for a management role.

The collaboration could include the adaption of the international entity's policies and procedures. Initial due diligence should take into account any local immigration, employment and visa issues.

Infrastructure Requirements

This covers equipment and operations and maintenance programmes.

It is important, for example, to ensure that obsolete or faulty equipment has not been provided by one of the parties and where equipment plays an important role, a survey of its condition has been conducted at the early stages.

IT

The legal arrangement should stipulate who pays for and implements upgrades and updates to IT.

Service Requirements and Standards/Performance Management

It is important to know what services are being delivered and by whom. This could be by reference to agreed service specifications and properly considered performance indicators that are capable of being monitored and measured.

Remuneration and Commercial Arrangements

It is vital that the remuneration and commercial arrangements between the parties are clearly described. Provisions could include a division of profits or a services related consultancy payment.

Changes and Variations Procedure

A procedure should be built into the collaboration to deal with any material changes and variations and the commercial consequences.

Termination and its Consequences

It is important to plan for the possibility the collaboration is not going to succeed, or that it is not successful.

Provisions should therefore be made for a clear set of events that could lead to termination and for dealing with the consequences.

These could include the return or re-engagement of staff, termination of the use of intellectual property or brand names, plus clearly stated financial consequences.

Hamid Yunis
Partner
London
hyunis@mwe.com

Hamid's global client base includes global health care providers, medical products manufacturers and organisations establishing "medical cities". Hamid advises on innovative structures for joint-ventures, public-private partnerships and the related funding arrangements.

Artificial Intelligence in Health Care: Framework Needed

DALE VAN DEMARK

The potential benefits of artificial intelligence technology are felt nowhere more fully than in the health care sector. Its integration into health care, is, however, fraught with technical, policy and regulatory challenges.

Although the incorporation of technology into human endeavours—commercial, political and personal—is a normal component of technological innovation, the advent of artificial intelligence technology is producing significant challenges we have not felt or understood with earlier innovations. For many years, for example, there has been speculation, research and public debate about the impact of the internet, the functioning of search engines, and online advertising techniques on commercial and political decisions.

The alleged "hacking" of the 2016 US presidential election, and the concerns about such activities in the 2017 European elections, will only heighten the interweaving discussions on free speech, national sovereignty, cyber security and the nature of privacy.

The use of artificial intelligence and machine-learning technologies has only added to the list of issues and areas of concern. The consequences of automobile accidents involving "self-driving" technologies, the "flash crashes" on securities markets due to algorithmic trading, and bias in systems designed to determine benefit eligibility, are requiring us to consider what happens when we defer judgment to machines, and highlighting the importance of quality in data sets and sensors.

THE GOVERNMENT IS COMING

Artificial intelligence legislation is currently rare, but governments are beginning to take note and take action. In 2016, the Obama administration convened working sessions and, ultimately, issued two reports on the impact of artificial intelligence. The UK Parliament's Science and Technology Committee issued a report on artificial intelligence around the same time. On 29 June 2017, a select committee on artificial intelligence was appointed in the UK Parliament, and in the United States a House of Representatives caucus has formed around artificial intelligence. At the same time, government agencies, such as the UK National Health Service and the US General Services Administration, are actively engaged in trying to harness the power of artificial intelligence.

While comprehensive legislation on artificial intelligence is non-existent, members of the European Union Parliament have called for EU-wide liability rules and the eventual recognition of legal status for artificial intelligence systems.

Behind these government forays is a vast dialogue in the marketplace of ideas where innovators, business leaders, scientists and others—including Elon Musk, Bill Gates, Jack Ma and Stephen Hawking—are lauding, warning and pontificating on the benefits and threats of artificial intelligence.

There is little doubt that artificial intelligence, as another form of automation, will reduce the number of current jobs; but debate continues over whether or not other work will be created in sufficient quantity to replace jobs that are lost. There is also little doubt that artificial intelligence, when "taught" badly, can exhibit bias resulting in sub-par or illegal performance; but whether or not this issue is systematically avoidable remains open to debate and fraught with the practical difficulties associated with data quality. Finally, the unregulated use of artificial intelligence throughout various sectors of the economy— resulting in the so-called Black Box Society—has many struggling to reconcile the efficiencies created by artificial intelligence with the apparent loss of control that goes along with it.

ARTIFICIAL INTELLIGENCE IN HEALTH CARE

Improvements in clinical pathways, administrative functions and therapeutic development processes through the use of artificial intelligence promise dramatic improvements in care quality and efficiency. Highly trained, machine-learning artificial intelligence systems are producing diagnostic results that, in some circumstances, are at the level of board certified physicians. Some are acting as the first point of contact between a patient and health care provider. Others are sifting through amounts of data that were previously thought impossible to review, in order predict conditions or to spot population trends.

In no other sector of society, however, are the concerns of artificial intelligence adoption more apparent and pressing than in health care. Licensed professionals, patients and their families, public institutions, private for-profit and not-for-profit organisations, researchers, insurers, regulators, educational institutions, entrepreneurs, investors, technology companies, insurers and other industry sectors all participate in health care delivery, payment and oversight, and each has its own perspective and interests.

This multiplicity of stakeholders, and the many ways in which artificial intelligence can be utilised, means that the issues associated with artificial intelligence will become apparent more quickly than in other, less regulated and less sensitive, industries.

Health Care Professionals

The role of health care professionals inevitably will evolve with the adoption of artificial intelligence. Diagnostic and consumer engagement tools are increasingly taking on the role of physician extenders, making deep incursions into the domain of the practice of medicine. These developments will challenge not only physicians themselves but also the boards and agencies that oversee their activity and conduct.

Issues that still need to be resolved include those around the responsibilities that physicians have when using this new technology, the rights of patients to demand the use of artificial intelligence tools in their treatment, whether or not physicians have a role in the development of artificial intelligence tools, and should they bear responsibility for the machine-learning protocols.

It is possible that in our lifetime medical schools may be required to include computer science courses to better prepare physicians to integrate artificial intelligence into their practices. Ultimately, if an artificial intelligence system is proven to perform at a higher level than an average physician, government and private payers for health care services may question the need for physicians at all.

“Diagnostic and consumer engagement tools are increasingly taking on the role of physician extenders.”

Patients

As artificial intelligence technology continues to advance, individuals will have greater information, and diagnostic and treatment options available to them, without physician mediation. While the positive aspects of these developments are indisputable, they do raise significant issues around the extent of individual responsibility in health care.

With greater tools available to individuals, questions arise as to how much we should expect individuals to do for themselves. Debates are currently taking place over the extent to which individuals can expect their physicians to be knowledgeable about the extent and quality of information the individual can deliver through, for example, wearable technology. In the future, access to high-functioning sensors and diagnostic tools may burden individuals with greater responsibility to care for themselves, particularly in the context of third-party payer programs.

Policy and Regulation

Beyond these questions related to physician and patient responsibility are significant policy questions. These include questions relating to how machine-learning artificial intelligence systems that are capable of rendering judgment previously reserved for licensed professionals should be regulated. Governments continue to struggle with how to regulate health-related software; artificial intelligence and machine-learning technologies will only make this struggle more difficult.

THE MISSING LINK

The health care industry is likely at the leading edge of the hard truths of the potential societal changes that come with artificial intelligence. Litigation will address some of these issues; but just as bad facts can result in bad case-law, bad case-law can subsequently result in bad public policy.

Thoughtful public discussion about artificial intelligence is happening now, and the use of artificial intelligence in health care is more apparent every day. Existing legal and regulatory frameworks are ill-equipped to welcome this new technology. Government regulation, informed by the various interests and with an eye on existing and future capabilities, can help set a rational framework that balances risk, innovation and patient safety.

Dale Van Demark
Partner
Washington, DC
dcvandemark@mwe.com

Dale advises clients in the health industry on strategic transactions and the evolution of health care delivery models.

Spotlight on China's Hospital System

DAVID DAI AND JENNY WANG

Hospitals in China differ greatly from those in the west with respect to their relationships with physicians and patients; but they also share some of the same legal challenges faced by western hospitals.

As of the end of 2016, China had approximately 29,000 hospitals, comprising 13,000 state-owned public hospitals and 16,000 private hospitals.

PUBLIC V PRIVATE HOSPITALS

There are two main categories of hospitals in China: state-owned public hospitals (including state-owned teaching hospitals that are affiliated with universities), and private hospitals that are either locally owned or have foreign investment. Although the number of private hospitals exceeds the number of public hospitals, public hospitals account for more than 80 per cent of market share by revenue.

Owing to various regulatory restrictions, the number of foreign-invested private hospitals is still very low, and they are typically located in large metropolitan cities and predominantly serve expatriates and the rising Chinese upper-middle class.

PHYSICIANS

Except for a small number of physicians who practice through private medical clinics, most Chinese physicians are employed by hospitals. Physicians are only permitted to practice medicine through a registered employer, as stated on their medical practice certificates, and they are typically registered to practice in only one medical institution. As part of the government's effort to encourage private investment in China's health care sector, recent policy changes are gradually allowing physicians to practice at multiple locations.

> "Chinese physicians employed by hospitals are not personally liable for medical malpractice."

It is also notable that Chinese physicians employed by hospitals are not personally liable to their patients for medical malpractice. Instead, hospitals, as the employers, are solely responsible for any medical negligence on the part of their employed physicians. This liability shield for physicians, and the general lack of trust in the legal system, have contributed to a rising level of violence against physicians, where aggrieved families are known to hire street criminals to assault medical staff for alleged medical negligence.

PATIENTS

In Most western countries, with the exception of emergency rooms, patients typically do not seek medical care directly from hospitals; instead, they are referred to hospitals by their attending physicians.

In China, patients go directly to a hospital for medical care, often waiting hours for a same-day appointment. Patients, rather than physicians, therefore choose the hospital. In urban settings where there are multiple competing hospitals, patients typically prefer large, state-run public hospitals.

PAYORS

Unlike the United States, for example, China offers universal health care coverage for a basic level of medical services. Some patients are also covered by private insurance through their employers.

Chinese hospitals also offer different levels of services and add-ons for an additional cost. For example, a basic room at most public hospitals holds three to six patients, whereas an upgrade to a private room (which would not be covered by insurance) could cost the equivalent of US$70 to US$150 per day.

SALE OF DRUGS AND MEDICAL DEVICES

Most Chinese hospitals participate in the national health care reimbursement program. The majority of drugs and medical devices used in hospitals that participate in the national reimbursement program are procured through a centralised bidding process *via* purchasing platforms managed by the government.

The government sets the prices for drugs and medical devices that are covered by the national reimbursement program, but allows hospitals to charge a mark-up of up to 15 per cent. This mark-up generates a significant portion of the operational profits of Chinese hospitals, which results in hospitals being heavily dependent on the sale of drugs and medical devices to finance their operations.

Payment for physician services under the national reimbursement program may not be marked up, and is relatively low. This has a negative impact on the overall income and welfare of Chinese physicians, who are not as well compensated as their counterparts in, for example, the United States. As a result, many Chinese physicians rely on kickbacks from pharmaceutical manufacturers or distributors, and cash gifts from patients, to supplement their income.

These two factors incentivise the overutilisation of expensive drugs, which has become a significant social issue in China. As part of its ongoing health care reform, the government has been addressing the payment issue by gradually allowing hospitals to set health care service prices according to the market, eliminating the mark-up on drugs and medical devices, and increasing enforcement against corruption and misconduct in the health care sector. Penalties now include administrative and even criminal sanctions.

LICENSING

Hospitals in China must have a wide range of licenses and permits from various health care, environmental protection, fire protection, tax, labour, construction, corporate and civil registration authorities. The statutory requirements for issuing these licenses and permits are often ambiguous and subject to the discretion of the government officials in charge. As a result, it is not uncommon for operators to bribe government officials in order to obtain and maintain practice licenses and permits.

REFERRAL FEES AND REIMBURSEMENT FRAUD

As the dominant player in the Chinese health care sector, state-owned public hospitals are able to attract the best physicians, nurses and other resources, which make them the preferred choice for patients. In contrast, private hospitals, including those with foreign investment, face significant challenges in attracting patients.

As a result, many private hospitals have had to make themselves more competitive, such as by offering free checkups, free food and pickup services, to attract patients. Others have turned to more aggressive, and arguably illegal, marketing efforts, such as paying referral fees to public hospital physicians to redirect patients to the private hospital, and offering improper discounts and kickbacks to patients.

It is also typical for private hospitals to augment medical expenses by increasing hospital stays, charging for nonexistent surgeries or medications, or excessive prescriptions. Some private hospitals have even been found to collect patient identification cards to create fraudulent medical records and reimbursement claims. These all contribute to a negative perception of private hospitals in China.

DATA PRIVACY

Where Chinese hospitals share the same challenges that face western hospitals is in relation to their data. They are required to comply with regulations relating to the management of medical records and maintaining a medical information management system. They are prohibited from disclosing patient medical records for any purposes other than treatment, education and research. Hospitals are also required to maintain an internal compliance program to ensure the confidentiality of various types of patient medical records.

Patients have a private right of action for any unauthorised disclosure of their medical information. It is also a criminal offense to sell or otherwise unlawfully disclose to third parties personal data collected by a medical professional in the course of providing medical services.

It is notable that certain population health information collected by Chinese hospitals, including demographic information and electronic medical records, must be stored on servers located within China. Moreover, there is a proposed regulation that would deem hospitals as operators of "Critical Information Infrastructure" under the recently enacted China Network Security Law, which would subject any cross-border transfer of patient medical information by to additional safety evaluation processes by government agencies.

David Dai
Partner, MWE China Law
Shanghai
ddai@mwechinalaw.com

Junda (David) Dai represents a variety of European and US health care clients in their direct investments in China's health care sector, including green-field investments, cross-border mergers and acquisitions, private equity investments and strategic alliances, and related privacy and data protection, licensure and other regulatory compliance issues.

Jenny Wang
Counsel
Los Angeles
jjwang@mwe.com

Jenny Wang focuses her practice on the transactional and regulatory aspects of the health care industry, such as complex hospital-physician integration and affiliations, mergers and acquisitions, joint ventures, fraud and abuse matters, and tax-exempt bond financings. She also has experience working in Shanghai, China, on cross-border corporate transactions.

Accountable Care in the United Kingdom: Learning From International Experience

SHARON LAMB

Many countries are turning to value based payment and accountable care models. Moving to a new model of care is not straightforward; having a clear plan that takes into account valuable lessons learned elsewhere will be vital.

Whilst different international health systems have different regulatory and legal systems, many face similar demographic and health care funding challenges. There is, for example, no straightforward answer to the conundrum of limited financial resources to accommodate an ageing population that has increasing health care needs.

In recent months, NHS England has renewed its new models of care and devolution programme and announced a fast track wave of eight accountable care systems (ACSs).

The ambition is to provide high quality care in the community, at home and in care homes; avoid unnecessary hospital admissions; shorten length of stay; enable patients to recover at home; and deliver longer term savings.

THE UK ACO OR ACS MODEL

Accountable care terminology originates in the United States, where accountable care organisations (ACOs) have grown in response to a need to control costs, reduce fragmentation and align incentives. There has been a long history of integrated care and delivery programmes in the United States, but changes in health care legislation provided key impetus to a growth in ACOs.

UK ACSs will have similar aims. They will be expected to integrate care between providers (primary, community, mental health and acute), likely using capitated or valued based payments with shared savings and risk. An ACS will have significant control over funding and will manage contractual relationships across a health system.

This all marks a major change, not least for providers, who have previously competed with each other with payments on a per service tariff. Some commentators have argued that, as in the United States, an ACS will need a statutory UK basis to achieve true success. The necessary change to NHS law, however, now looks unlikely given the amount of parliamentary time devoted to implementing Brexit. An ACS in the United Kingdom will therefore need to be set up within an existing system, using flexibilities where they exist. Valuable lessons can be learned from similar models in other countries.

MAXIMISING THE CHANCES OF AN ACS SUCCEEDING

- **The right organisational and governance structure:** An ACS will need a contractual or corporate governance form that works within existing law, balances the competing interests of different providers, and provides for a response to breaches by a provider, such as deviations from agreed clinical pathways and protocols. In addition, some level of independence is needed to deliver impartiality and co-operation in an ACS. This has shown to be a sticking point for providers, and agreeing a model that allows for independence and impartiality is not straightforward. Some corporate forms have also faced technical issues, mainly around taxation and the powers of public bodies. As a consequence, some ACS models are based on prime or contractual models which, in turn, can raise questions about how the prime provider will be held to account.
- **Capital and investment:** Whilst ACS models are partly a response to funding constraints, experience elsewhere shows that if integrated delivery models focus only on immediate cost savings, longer term savings may suffer. This is because

> Strong leadership and contractual governance will be essential.

the early years of an ACS will require investment in primary, community and preventative care measures. A key issue will be ensuring that ACSs have access to private or public funding to develop the right infrastructure and systems.

- **Information and electronic patient records:** In order to be able to respond quickly to care needs, it is almost inevitable that providers will need to move to real time patient data and population tools. This will likely include a shared electronic patient record that allows patients to communicate with the ACS, and providers within the ACS to respond to each other and to facilitate data analysis.
- **Patient choice:** Patients must be able to choose or move between providers. Many ACS models will cover large geographic areas and, whilst there is a temptation to move to large monopoly providers, ACS systems will need to be lawful, comply with the NHS Constitution, and not limit the ability of patients to choose alternative providers, especially where quality may not be improving or there are long waits for care.
- **New contractual models, skills and leadership:** Moving to value based and shared savings models will require skills and experience that are different to those currently found in the sector. This issue is often under-estimated. Key new skills will be needed including in relation to population analytics, management and risk stratification, information technology, and payment models contractual and payment models.

Strong leadership and contractual governance will be essential to encourage providers to work together in a new way.

Sharon Lamb
Partner
London
slamb@mwe.com

Sharon is recognised for her knowledge and understanding of the health care legal landscape, including in-depth understanding of NHS law and policy.

Learn More

Visit www.mwe.com/experience to learn more about our Firm's capabilities. To subscribe or update personal email subscriptions from McDermott, visit www.mwe.com/subscribe.

Our publications are all accessible from www.mwe.com and include:

- *ANDA Update*
- *Antitrust M&A Snapshot*
- *China Law Alerts*
- *Focus on China Compliance*
- *Focus on Private Equity*
- *Focus on Tax Strategies & Developments*
- *Inside M&A*
- *IP Update*
- *Korea Quarterly*
- *Managing the Transition to Transformation*
- *On the Subjects*
- *Special Reports*
- *UK Employment Alerts*

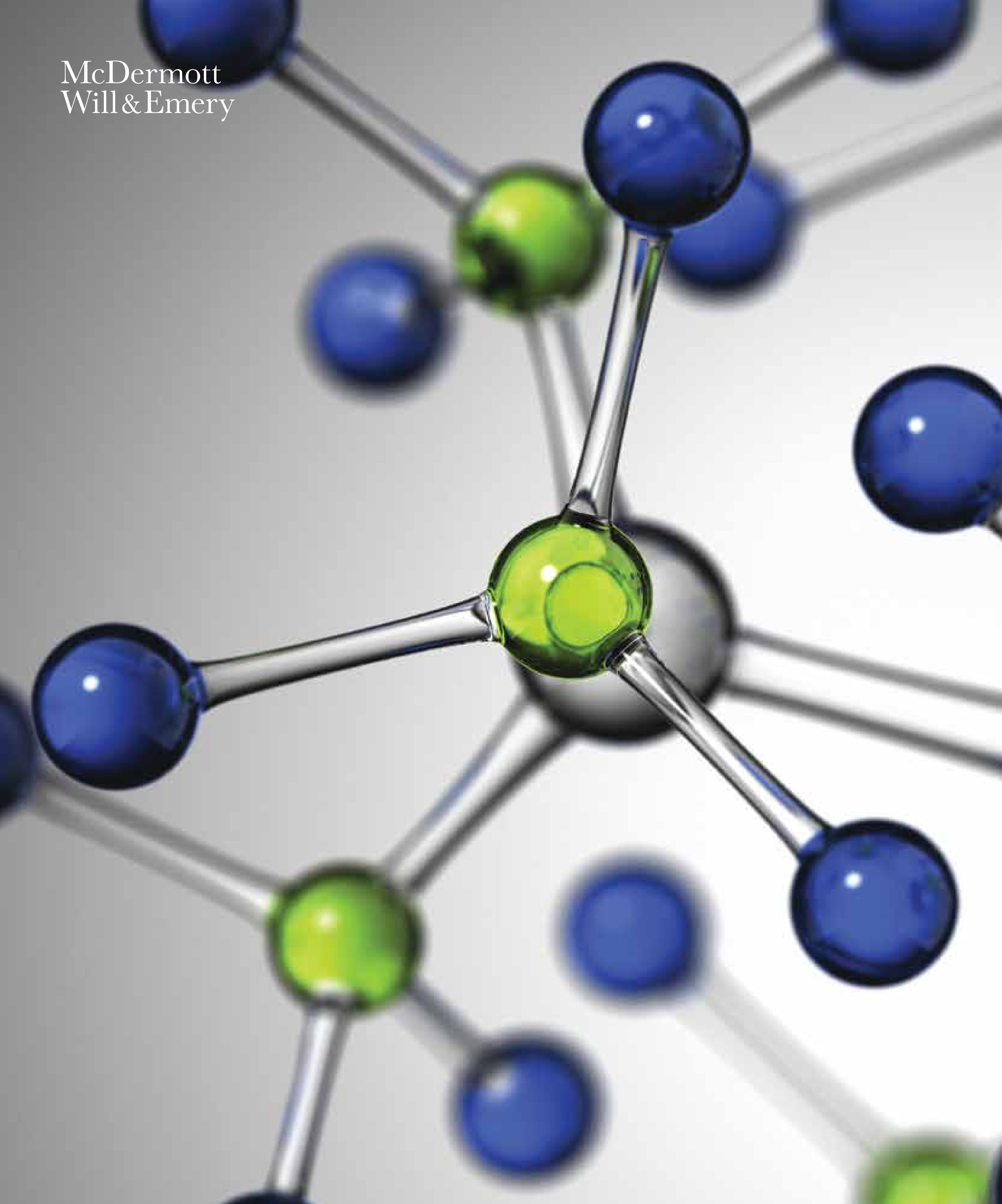
Stay connected on business issues and visit McDermott's blogs:

- www.alcohollawadvisor.com
- www.antitrustalert.com
- www.corporatedealsource.com
- www.employeebenefitsblog.com
- www.energybusinesslaw.com
- www.fcaupdate.com
- www.insidesalt.com
- www.ofdigitalinterest.com
- www.taxcontroversy360.com

IRS Circular 230 Disclosure: To comply with requirements imposed by the IRS, we inform you that any US federal tax advice contained herein (including any attachments), unless specifically stated otherwise, is not intended or written to be used, and cannot be used, for the purposes of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter herein.

International News is intended to provide information of general interest in a summary manner and should not be construed as individual legal advice. Readers should consult with their McDermott Will & Emery lawyer or other professional counsel before acting on the information contained in this publication.

©2017 McDermott Will & Emery. All rights reserved. Any use of these materials including reproduction, modification, distribution or republication, without the prior written consent of McDermott Will & Emery LLP, is strictly prohibited. This may be considered attorney advertising. Prior results do not guarantee a similar outcome.



www.mwe.com/international/