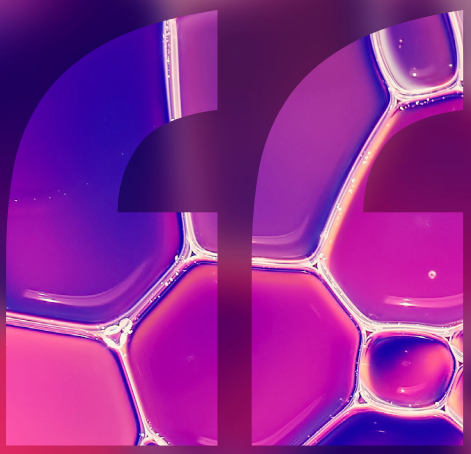
CLIFFORD
CHANCE



ESG AND COMPLIANCE CHALLENGES FOR THE HEALTHCARE SECTOR

— THOUGHT LEADERSHIP

OCTOBER 2024

ESG AND COMPLIANCE CHALLENGES FOR THE HEALTHCARE SECTOR

Increasingly complex regulatory, governance and compliance challenges across the globe are presenting new legal risks for the healthcare sector. In this update from a recent client event held by Clifford Chance's Healthcare & Life Sciences practice group we explore how our clients can respond to these challenges in a risk-based way.

Sustainability and ESG in healthcare - US and EU perspectives

"In the US, we're finding that companies are coalescing around the term sustainability rather than ESG as it focuses on the purpose to manage the enterprise in a way that's designed to serve the long term," says Washington D.C.-based Partner Steve Nickelsburg. The sustainability reports produced by a number of major pharmaceutical and medical device companies touch on a range of environmental sustainability topics such as greenhouse gas emissions, product packaging and water and waste management; social issues such as supply chain integrity with respect to modern slavery, conflict minerals and human rights; and ethics and governance. "One topic that is unique to the healthcare sector is equitable access and affordability, and we see that featured prominently," says Nickelsburg. "The pharma and medical device industries are unique in that they tend to put environmental issues last in their sustainability reports. Companies in the sector put equitable access and supply chain risk – including modern slavery risk and geopolitical risks associated with sourcing supplies – first," he says.

"Each of these topics present important substantive risks that need to be managed, as companies are facing detailed sustainability reporting requirements." Europe is taking the lead with the Corporate Sustainability Reporting Directive (CSRD), with increased requirements for net zero transition plans, and with substantive diligence requirements, for example through the Corporate Sustainability Due Diligence Directive (CSDDD).

Nickelsburg adds that with respect to investments in the sector, "given the current landscape, companies need to broaden their scope and ask for non-financial disclosures such as sustainability reports or other non-financial disclosure reports, look at representations being made in annual reports, and have all of those reviewed by people who are attuned to the risks because this is no longer a simple box-ticking exercise. We're dealing not solely with hard law – in many cases it's soft law, expectations and reputation, and therefore assessing those risks requires some judgement. You may find in a target that if sustainability teams are not closely aligned with their legal teams, one being more prone to aspirational statements and the other prone to more looking at things through a risk management lens, that there are risks or gap areas that haven't yet been identified. Diligence and risk assessment requires a more nuanced lens."

Greenwashing is a major risk – the Australian Perspective

Greenwashing – making misleading or false claims about a company's environmental impact, products or services – is an increasing risk as companies are held to account for the accuracy of their claims by NGOs, consumers and the media.

In Australia, two enforcement authorities – the Australian Competition and Consumer Commission (ACCC) and the Australian Securities and Investment Commission (ASIC) – are taking a keen interest in this issue. So far, ASIC has brought three enforcement proceedings in relation to greenwashing claims in the financial services sector, one of which has resulted in a fine of AUD11 million dollars. ACCC

has brought one proceeding so far. This concerns alleged greenwashing in relation to claims on the packaging of a laundry product which say that the recycled plastic used comes from ocean-based plastics.

“Packaging should be on the radar of healthcare businesses in this jurisdiction because packaging rules in Australia are currently subject to reform,” says Naomi Griffin, a Clifford Chance Partner based in Sydney. There is a consultation underway on new regulations that will underpin the Recycling and Waste Reduction Act 2020. This will require packaging to comply with national packaging design standards so that all new packaging will be reusable, recyclable or compostable and will prevent the use of listed chemicals of concern and lead to a circular economy for packaging. “It’s not just about waste reduction, but also potential health and economic benefits and the reduction of impacts on human environmental health." Griffin says.

Anti-Money Laundering – new laws in Singapore with extraterritorial reach

Following a series of high-profile anti-money laundering cases, Singapore has introduced a new Anti-Money Laundering and Other Matters Act to enhance existing laws and increase prosecution power. The amendments to current legislation include provisions which enable the investigation and prosecution of money laundering offences when it is suspected that funds are derived from serious environmental crimes that are committed overseas. “This means that corporations – including those in the healthcare sector – will need to ensure that their business activities and operations do not contravene environmental laws, including the illegal processing or disposal of hazardous waste,” says Janice Goh, a Partner at Cavenagh Law, a formal law alliance partner firm of Clifford Chance.

Data in healthcare privacy and cybersecurity

“Healthcare is all about sensitive patient data – and protecting it. A recent survey indicates that 10% of around 3,000 cyberattacks in 2023 targeted the health industry and the risk is increasing,” says Torsten Syrbe, a Clifford Chance Partner based in Düsseldorf and co-chair of the firm’s healthcare and life sciences sector group.

Globally, cyberattacks involve software vulnerabilities, malware or hardware problems such as lost or stolen back-up tapes that have led to data breaches. These types of attacks have played out in a number of ways and have an impact on regulation, litigation and corporate reputation and consumer trust.

In Australia, Medibank, a large private health insurer, was hacked 2020. The personal information of 9.7 million Australians was stolen and released on the dark web, including passport numbers, health claims, treatment types and birth dates. “From a regulatory perspective, there was scrutiny from a number of angles,” says Griffin. The Office of the Australian Information Commissioner has powers to investigate complaints by consumers and can require compensation to be paid. It’s currently investigating representative claims by at least one, and possibly two, cohorts of Medibank customers.

Meanwhile, the Australian Competition and Media Authority has jurisdiction to penalise companies for data breaches with fines of up to AUD50 million (approximately EUR 30 million) for serious or repeated breaches. In addition, ASIC focuses on the perspective of directors’ duties and the ASIC Commissioner also looks at directors’ duties and whether there are adequate systems and processes in place to prevent data infiltration.

Litigation is a particular risk. Within a year of the Medibank breach, and, separately, following a breach at Australian telecoms company Optus in which 10 million customers had personal data stolen in a cyberattack, a number of class actions have started. As Medibank is an ASX listed company, the lead claim took the form of a stock drop case, and that claim alleges that in statements to the market between 2016 and 2022, Medibank said it had effective systems and processes in place to monitor and deal with cyberattack risk, whereas it’s alleged that

it did not and that Medibank engaged in misleading or deceptive conduct under the Corporations Act, with the result that its share price was inflated.

Such breaches have a significant impact on corporate reputation and consumer trust. “Medibank saw its share price fall, and it lost a huge number of customers in the first month. It was on the front pages of the newspapers for weeks, and over the last two years it has had to do a lot to win back consumer confidence. Data security is a risk area that’s particularly acute for the healthcare industry. However, it is a risk that can be managed,” says Griffin.

Data risks in healthcare products and services

Many healthcare products and services have already launched e-services including healthcare apps, virtual doctor’s appointments, online pharmacies and wearable health trackers that collect data on the user’s fitness levels, heart rate, sleep and mental health. “When rolling out such apps or services healthcare providers should be mindful of the type of personal data that it collects via the app and to ensure that consent, if required, is validly provided,” says Goh. “For example, if there are ads and third-party marketing provided on the app, consent from the individual to provide their data to third parties must also be obtained insofar as it is required under applicable law.”

Companies should also consider whether an app or service coupled with fitness or health-tracking devices could result in the product being a medical device or service under healthcare regulations which require necessary regulatory approvals. “Companies should also consider whether the data that is collected from the user for purposes of the app or e-service falls under personal protection laws only, or does it also fall under specific laws in relation to patient data, or both? Healthcare laws in relation to patient data and general personal data protection laws may intertwine, and a relevant data-mapping exercise must be conducted in relation to that specific product,” Goh says.

Healthcare – AI and governance

The EU AI Act, which came into force in August 2024, is a framework regulating AI in a cross-border approach in all European Member States, and it comes with a risk-based approach, so the higher the risk related to an AI solution, the more obligations for the relevant operators. “In principle, it splits the responsibilities between different parties operating AI systems in various roles. So, for example, for providers, for distributors, for deployers or importers,” says Gunnar Sachs, a Partner in Clifford Chance’s global Healthcare & Life Sciences practice and co-head of the firm’s global Healthtech Group, based in Düsseldorf.

In Germany, providers, for example, need to meet extensive new obligations requiring specific procedures documentation, obligations, control mechanisms and so on. Deployers of AI systems, by contrast, must comply with monitoring and transparency obligations, while distributors must check that the software incorporating the AI solution carries the required conformity markings and is actually accompanied by the required documentation. Last, but not least, importers must ensure that the AI providers themselves have carried out the required conformity assessments on their relevant systems. “AI requires compliance with specific requirements and prerequisites. It requires the implementation of a risk management system, it requires to have in place a data and data governance system, it also requires documentary record-keeping systems to be in place, it requires human oversight and it requires compliance with transparency requirements,” says Sachs. “So, how do you assess and monitor AI on an existing governance organisation, and how can you use the existing compliance governance that you might have already in place?” he says.

Managing AI risk

Peter Dieners, a Düsseldorf-based Partner with decades of experience in healthcare compliance, says that it is important to understand what governance means – and what it does not.

"We know that what many 'traditional' risks, such as anti-bribery and corruption, competition-related risks and others, have in common is that an organisational framework has to be designed which aims that any incident can be qualified as an outlier and not be traced back to structural failure. Now we are asking ourselves, what does this mean in terms of AI? Of course, there are many obligations in the EU AI Act, but they are not really related to the question, how do I have to organise my organisation and my management system?"

The EU AI Act says that every company needs to establish a risk assessment and to implement a risk management system, but it does not further specify the details regarding the required method of the risk assessment and the necessary elements of the risk management system. There are some helpful benchmarks, best-practice examples and rules available for setting up compliance governance systems, for example, ISO standard 37000. It is not related to AI risk; in particular, it can also be used to set up a risk management system to avoid corruption or competition antitrust risks.

"An AI governance system is similar to other risk management systems which companies have implemented for many years. For instance, when it comes to corruption, there are seven, 10 or 12 elements of a functioning or robust compliance governance system, depending on how you count them. These governance systems are related to corruption and fraud, healthcare fraud and abuse risks," says Dieners. "The modules are very similar for AI. First, it's important to determine an AI strategy and the principles, values and objectives. It's important that there's board accountability for setting and monitoring the overall strategy in using AI and providing direction for governance on the use of AI. For instance, it's important to delegate the duties of the board to particular functions – this may be the compliance officer, sustainability officer or an AI officer managing the risk management system."

He adds that it is sensible to create a committee which could involve representatives from legal, compliance, risk management, product development, marketing risk and customer service to take a holistic view of the risks, set up rules for audits, put appropriate training in place as well as corrective actions and sanctions in the event of non-compliance. "And last but not least, it's really important to have the right third-party management in place and rules for the engagement of and monitoring of third-party vendors."

Summary

"What risks are we seeing across the globe? What is it about these risks that keeps board members and general counsel up at night?" asks Syrbe. "It is clear that there are three key themes that emerge for compliance teams from a broad variety of sectoral challenges – (i) new sustainability and ESG requirements in Continental Europe and the US, (ii) more countries introducing strict anti-money laundering regimes, such as Singapore, and (iii) data privacy, cybersecurity and AI all requiring additional internal governance and leading to more external scrutiny worldwide.

We often recommend that our clients "Think globally. Act locally". This continues to be relevant advice as we see jurisdictions across the globe grapple with the regulatory challenges presented by new technologies. It is helpful to be able to see regulatory efforts in a global context, but it is as important as ever to be on the lookout for specific regulatory developments in relevant jurisdictions to be able to assess the impact on operations at the local level.

To this guidance, we can now add "Engage holistically. Respond incrementally." An organisation-wide, and multi-disciplinary, approach will ensure our clients can draw on their in-house experts to respond to new challenges in this space – and to do so leveraging governance mechanisms that are already functioning well in their organisation.

CONTACTS

Torsten Syrbe Co-Chair, Healthcare & Life Sciences Sector Group
Dusseldorf
T: +49 211 4355 5120
E: torsten.syrbe@cliffordchance.com

Naomi Griffin
Partner
Sydney

T: +61 2 8922 8093
E: naomi.griffin@cliffordchance.com

Steve Nickelsburg
Partner Washington DC

T: +1 202 912 5108
E: steve.nickelsburg@cliffordchance.com

Peter Dieners
Partner
Dusseldorf

T: +49 211 4355 5468
E: peter.dieners@cliffordchance.com

Gunnar Sachs
Partner
Düsseldorf

T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Janice Goh
Partner, Cavenagh Law Singapore

T: +65 6661 2021
E: janice.goh@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

JOB0000019140