

Grip • Health

SPECIAL
ISSUE

HEALTHCARE'S COMPLIANCE CHALLENGE

Industry experts discuss
the future of risk, data,
innovation and regulation



GRIP magazine showcases the coverage that can be found on our digital information service, Global Relay Intelligence & Practice. It is aimed at decision makers working at enterprise corporations, financial services firms (especially banks, brokers, and asset managers), and in the insurance, commodities, healthcare and life sciences sectors.

It covers the interconnected relationship between Technology, Risk, and Compliance (TRC). It delivers insights on developing technology, key risks that need recognition, best practice, and the most effective methods to ensure compliance.

Global Relay has been providing compliance technology for more than 25 years. GRIP is an opportunity to showcase the deep subject matter expertise developed during this time. GRIP is made available in print and digital format to customers, prospects, and partners of Global Relay.



GRIP magazine, a Global Relay publication, is owned and operated by Global Relay Communications Inc. (“Global Relay”). Global Relay carries out business in Canada, the United States and internationally under the Global Relay name.

This publication is provided for general information only. This publication is not intended to be legal, financial, investment, tax, regulatory, business or other professional advice, and should not be relied upon as such. It is important to seek independent advice from a qualified professional for all inquiries regarding such matters. While reasonable efforts have been made to ensure that the information contained within this publication is accurate, Global Relay makes no warranty, representation or undertaking of any kind whatsoever, whether expressed or implied, nor does it assume any responsibility, for the quality, accuracy, completeness, or usefulness of any information contained within this publication. Global Relay will not be liable for any direct or indirect, incidental, consequential, special or punitive loss or damages arising out of or in connection with the use of or reliance on the information contained in this publication.

Unless otherwise stated, the material published within GRIP magazine is owned by, or licensed to, Global Relay and is protected by copyright, trademark and other intellectual property laws of Canada, the United States, and international treaties. Any reproduction, modification, distribution, transmission, republication, display, or performance, in whole or in part, of any materials in this publication is prohibited without the express written permission of Global Relay. Inclusion of GRIP magazine materials in newsletters, magazines, books, and on other sites is subject to express written permission from Global Relay.

Grip. Health

Publisher

Alex Viall

Managing Editor

Martin Cloake

US Content Manager

Julie DiMauro

Editorial consultant

Richard Cree

Designer

Nikki Ackerman

Cover photography

Getty Images

Contributors

Alexander Barzacanos

Thomas Hyrkiel

Jean Hurley

Martina Lindberg

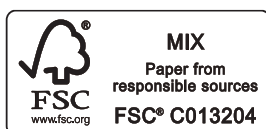
Scott A Memmott

Hameed Shuja

Jonathan P York

Printing

Geoff Neal Group



This publication has been printed by the Geoff Neal Group on sustainable, FSC®-certified paper made from trees from well-managed forests and other controlled sources. All coatings used in the making of this magazine are water-based. All inks used in the making of this magazine are vegetable-sourced. Geoff Neal Group recycles the chemicals it uses in this process and also any waste that is a result of the production process.

Copyright © 1999 - 2025
Global Relay Communications Inc.
All Rights Reserved.

“

Any discussion of our overall health should include a thoughtful examination of what makes us happy”

T

his special edition of GRIP has healthcare as its focus and contains a wealth of articles, interviews and deep dives into a variety of healthcare subsectors and topic areas. We look at issues ranging from conflicts of interest to third-party risk management, as well as cybersecurity challenges – all in a sector where compliance challenges are becoming more complex. And we’ve spoken to some of the sector’s thought leaders too, gathering some fascinating insight.

The magazine does not specifically mention mental health, though, and it is with that in mind that I write this editorial. If left unaddressed, mental health inequities could lead to about \$14 trillion in excess costs between now and 2040, according to one analysis of the topic. In far more general terms, there is a lot to be said for our daily mental wellbeing that may or may not involve medicine and therapy – but greatly affects our lives. And there might be some glimmer of hope for our overall mental states if we account for the impact of caring and sharing on our own happiness.

The latest issue of the World Happiness Report offers a lot to smile about. For example, when researchers dropped wallets in the street to find out what proportion of people returned them to their owners, it was far higher than expected. And benevolence increased during COVID-19 in every region of the world. This “benevolence jump” has been sustained since then, with benevolent acts still hovering 10% above their pre-pandemic levels.

Interestingly, our wellbeing depends on our perception of other people’s benevolence, as well as their actual benevolence. Since we underestimate the kindness of others, our wellbeing can be improved by receiving information about altruism.

Any discussion of our overall health should include a thoughtful examination of what makes us happy – and it turns out that making other people happy does the trick well.

We wish you much happiness extended and received.



Julie DiMauro

Julie DiMauro

US Content Manager

Complete the circle

Compliance is complicated,
you need a trusted partner,
not another vendor



25 years of innovation



Integrated solutions



Regulatory expertise



Single vendor efficiency



24/7 support



Unmatched security

Complete communications compliance |  **globalRELAY.**

Contents



FEATURES

- | | |
|-----------|--|
| 10 | Jeff Lemay
Jazz Pharmaceuticals' CCO in conversation about the road ahead for compliance and legal teams in the sector |
| 12 | McKinsey's OxyContin settlement
Revelations about a moral and ethical void at a leading pharma firm provide lessons about consultant culture too |
| 14 | Risk as a catalyst
Technology is transforming how compliance judges the speed and effectiveness of risk response, says PwC's Tiffany Gallagher |
| 16 | Denis Jacob
The Ethics and Compliance Business Partner at Henry Schein on why compliance professionals need to think differently |
| 20 | India's pharma future
The country has built a dominant position as 'the world's pharmacy' but now faces a number of key challenges |
| 22 | Compliant growth in biotech
How smaller pharma and biotech firms can reduce compliance risks |
| 26 | Aaron Narva
The Founder and CEO of Confluxis on how his tech is being used to handle huge quantities of data to detect conflicts of interest as healthcare firms scale their business models |
| 30 | Overseeing AI
Legal experts from Morgan Lewis assess the risks and opportunities AI offers to the healthcare and life sciences sector |

SPOT ACTIONS

6-9

Notable enforcement case settlements from the US and Europe.

IN NUMBERS

34

The figures that illustrate the rise in healthcare data globally



ENFORCEMENT SPOT ACTIONS

New healthcare rules and regulations in New York State; Pfizer and Novo Nordisk rebuked; a ruling on patient data confidentiality; and an update from the UK CMA in our roundup of the latest enforcement actions.

JUILE DIMAURO
& JEAN HURLEY



NEW IN NY: DATA BREACH NOTIFICATION AND NEW HEALTH INFO PRIVACY LAW

New York State recently announced a settlement with financial technology and online financial services provider PayPal, Inc, over what it called PayPal's "inadequate training processes for key personnel in handling sensitive customer information."

The state also updated its breach notification law to revise timing and notice provisions and expand the scope of what constitutes "private information."

And a new bill is also about to be signed into law. The New York Health Information Privacy Act takes what its supporters say is a major step forward in protecting personal health data, by making it illegal for certain entities to sell an individual's regulated health information without explicit consent of the individual.

NYDFS settles with PayPal

New York State Department of Financial Services (NYDFS) Superintendent Adrienne Harris recently announced that PayPal, Inc will pay a \$2m penalty to New York State for violations of NYDFS's Part 500 Cybersecurity Regulation. An investigation determined PayPal failed to use qualified personnel to manage key cybersecurity functions and failed to provide adequate training to address cybersecurity risks. These failures led to sensitive customer information, including social security numbers (SSNs), being left unredacted and easily accessible to cybercriminals, the agency said.

NYDFS alleged that customer data was exposed after PayPal implemented changes to existing data flows to make IRS Form 1099-Ks available to more of its customers. However, the teams tasked with implementing these changes were not trained on PayPal's systems and application development processes.

As a result, they failed to follow proper procedures before the changes went live. This allowed cybercriminals to leverage

compromised credentials to access Form 1099-Ks, which included sensitive customer data, including SSNs.

The agency said its investigation also revealed that PayPal failed to implement and maintain written policies that addressed access controls, identity management, and customer data, and failed to use effective controls to protect against unauthorized access to Nonpublic Information or Information Systems.

Notably, the company did not require customers to use multifactor authentication or use controls such as CAPTCHA or rate limiting to help prevent unauthorized access.

NYDFS said PayPal had since remediated these issues and improved its cybersecurity practices.

NY data breach notification

New York Governor Kathy Hochul recently signed into law two bills (S2659B and S2376B) to modify and enhance the state's data breach notification law.

The amendments revise the timing requirements for notice to affected individuals, expand the list of regulators to be notified of the breaches, and add new data elements to New York's definition of "private information."

Timing: The amendments change the required notification to affected New York residents from "in the most expedient time possible and without unreasonable delay" to "no later than 30 days after discovery of the breach, except for the legitimate needs of law enforcement." This change was effective December 21, 2024.

Additional regulator notice: The law now requires notice to the NYDFS instead of just to the New York State Attorney General, the New York Department of State, and the Division of State Police. This was also effective on December 21.

Definition of 'private information': As of March 25, 2025, the definition of "private information" subject to the law's notification requirements will include:

◆ Medical information (for example, any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional);

◆ Health insurance information (for example, an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual or any information in an individual's application and claims history, including, but not limited to, appeals history).

In line with the Health Insurance Portability Accountability Act (HIPAA) exemption, a breach of protected health information wouldn't trigger additional notification requirements to affected individuals. But it requires notice to regulators, including the New York State Attorney General, the New York Department of State, and the Division of State Police.

New York Health Information Privacy Act

The recently proposed New York Health Information Privacy Act (NYHIPA), Senate Bill S929, awaits Governor Hochul's signature, and seeks to enhance the state's approach to protecting personal health data in the digital age.

The bill aims to establish stronger privacy protections and restrict health-related data being used or sold without explicit user consent. Supporters see it as a necessary evolution of data privacy laws, addressing gaps in federal regulations such as the HIPAA and responding to growing consumer concerns.

New York's legislation is notable for broadly defining what constitutes "regulated health information." Unlike HIPAA, which primarily governs hospitals, insurers, and healthcare providers, NYHIPA extends its scope to include any company that collects health-related data from New York residents. This means that digital health apps, wellness platforms, and employers offering health benefits could be subject to its requirements.

Unlike other state privacy laws that largely apply solely to residents of that state, NYHIPA imposes significant burdens on companies located in New York because it applies to the covered health information they process, regardless of whether the individual is located in or outside of New York. The Act will take effect a year after the governor signs it into law. ●

PFIZER AND NOVO NORDISK REBUKED OVER PHARMA PAYMENTS

US and UK authorities are monitoring pharmaceutical spending and disclosure in their respective jurisdictions, seeking transparency in the payments pharmaceutical companies make to the healthcare sector.

Payments covered include those made to patient groups, healthcare associations, charities, and training providers.

Pfizer's \$60m to DOJ

The US Department of Justice (DOJ) has announced that Pfizer Inc, on behalf of its wholly-owned subsidiary Biohaven Pharmaceutical Holding Company Ltd, has agreed to pay \$59,746,277 to resolve allegations that, prior to Pfizer's acquisition of the company, Biohaven knowingly caused the submission of false claims to Medicare and other federal healthcare programs, by paying kickbacks to healthcare providers to induce prescriptions of Biohaven's drug, Nurtec ODT.

The anti-kickback statute prohibits offering or paying anything of value to induce the referral of items or services covered by Medicare, Medicaid, TRICARE, and other federal health care programs. The statute is intended to ensure that medical providers' judgments are not compromised in any way by improper financial incentives.

Paying providers

The DOJ alleged that Pharmaceutical Holding, from March 2020 through September 2022, selected certain healthcare providers to be part of a group to promote its drug Nurtec ODT, a migraine treatment. These providers were given paid speaking opportunities and meals at high-end restaurants with the intent of inducing

them to prescribe Nurtec, the DOJ said. The kickbacks ended once Pfizer terminated Biohaven's Nurtec speaker programs upon its acquisition of the company, the DOJ confirmed.

"The settlement relates to alleged conduct at Biohaven before Pfizer's acquisition of the company in October 2022 and does not include any admission of liability or wrongdoing," a Pfizer spokesperson said. "We are pleased to put this legacy matter behind us, so that we can continue to focus everything on the needs of patients."

Novo Nordisk rebuked

Meanwhile, in the UK, alleged payments by a pharmaceutical company involved the maker of the popular blockbuster weight-loss drug, Wegovy.

The Prescription Medicines Code of Practice Authority (PMCPA), the UK's pharmaceutical watchdog, has reprimanded Wegovy maker Novo Nordisk for failing to correctly disclose dozens of payments over seven years to pharmacy firms, obesity charities, training providers, professional bodies, and patient groups.

The Danish drug giant, one of Europe's most valuable listed companies, systematically misreported, under-reported or did not disclose such funding, and even after admitting to errors and conducting an internal review, it failed to accurately report its spending.

The company has now been formally reprimanded by the PMCPA, which said it had brought the industry into disrepute. Finding 48 breaches of the industry code, the PMCPA said serious compliance failings – committed while Novo Nordisk was already the subject of an audit over prior breaches – "raised questions about the culture of the company and demonstrated poor governance and a lack of care."

The alleged breaches included £183,000 (\$228,700) in undeclared funding to a weight-loss-coaching company that partners with pharmacies and the NHS, sponsorship of webinars provided by a medical training provider, and grants to charities and a royal college. A payment of £338,435 (\$423,014) to a global obesity center was also incorrectly disclosed.

New investigations

The firm had previously admitted failing to correctly disclose payments, telling the PMCPA in 2023 that it had omitted more than 500 transactions worth £7.8m »

\$60m

The amount Pfizer paid the DOJ to settle claims against a subsidiary

(\$9.75m) to more than 150 organizations between 2020 and 2022.

The new, undisclosed payments came to light after an investigation by academics in the UK and Sweden, who cross-referenced transparency disclosures by Novo Nordisk with financial statements and other records from UK healthcare organizations.

The investigation by researchers at Bath and Lund universities, which overlapped with the PMCPA probe, found that even after conducting an internal review and claiming to rectify the issue, Novo Nordisk failed to accurately record further payments totaling £635,000 (\$793,070) to 30 organizations.

Previously, allegations in news reports detailed how Novo Nordisk paid experts who went on to promote its drugs in media appearances without always making their financial interests clear.

Sanctions

There is no legal requirement for companies to disclose payments to the healthcare sector, but many subscribe to an industry code that requires them to report through a voluntary scheme called Disclosure UK.

Disclosure UK is an industry-led initiative to deliver a searchable database that shows payments and benefits made by the pharmaceutical industry to doctors, nurses, and other health professionals and organizations in the UK.

Alleged breaches are assessed by the PMCPA, which can impose sanctions, including a public reprimand or requiring the company to publish a corrective statement. It can also report the company to the Association of the British Pharmaceutical Industry board, which may suspend or expel the firm from the association. ●



Effective cybersecurity includes knowing who has access to electronic protected health information”



HHS SETTLES HIPAA SECURITY RULE INVESTIGATION WITH HEALTH FITNESS CORP

The US Department of Health and Human Services' (HHS's) Office for Civil Rights (OCR) announced a settlement with Health Fitness Corporation, a company that provides wellness plans to clients across the country, to resolve a potential violation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.

The rule requires administrative, physical, and technical safeguards to ensure confidentiality, availability, and security of health information.

Under the terms of the resolution agreement, Health Fitness agreed to implement a corrective action plan that OCR will monitor for two years and has paid a penalty of \$227,816 to OCR. Health Fitness committed to ensure compliance with the HIPAA Security Rule and better protect the security of electronic protected health information (ePHI).

OCR enforces the HIPAA Privacy, Security and Breach Notification Rules, which set forth the requirements that covered entities (health plans, healthcare clearinghouses, and most healthcare

providers), and business associates such as Health Fitness must follow to protect the privacy and security of ePHI.

The HIPAA Security Rule establishes national standards to protect and secure the US healthcare system by requiring administrative, physical, and technical safeguards to ensure the confidentiality, integrity, availability, and security of electronic PHI (ePHI).

The Risk Analysis provision of this rule requires a regulated organization to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by that organization.

The settlement resolves OCR's investigation of Health Fitness, which OCR initiated after receiving four self-reports from Health Fitness over a three-month period of breaches of unsecured protected health information.

Health Fitness filed the breach reports on behalf of multiple covered entities as their business associate.

The wellness firm reported that, beginning approximately in August 2015, ePHI became discoverable on the internet and was exposed to automated search devices (web crawlers) resulting from a software misconfiguration on the server housing the ePHI.

Health Fitness discovered the breach in June 2018, initially reporting

that approximately 4,304 individuals were affected and later estimated that the number of individuals affected might be lower.

OCR's investigation determined that Health Fitness had failed to conduct an accurate and thorough risk analysis until January 2024 to determine the potential risks and vulnerabilities to the ePHI it held.

"Conducting an accurate and thorough risk analysis is not only required but is also the first step to prevent or mitigate breaches of electronic protected health information," said Anthony Archeva, OCR Acting Director. "Effective cybersecurity includes knowing who has access to electronic health information and ensuring that it is secure."

In addition to agreeing to pay the fine and to hire a compliance monitor, Health Fitness committed to take steps to ensure compliance with the HIPAA Security Rule and protect the security of ePHI by:

- ◆ annually reviewing and updating as necessary its risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;

- ◆ developing and implementing a risk management plan to address and mitigate security risks and vulnerabilities identified in its risk analysis;

- ◆ implementing a process for evaluating environmental and operational changes that affect the security of ePHI;

- ◆ developing, maintaining, and revising, certain written policies and procedures to comply with the HIPAA Privacy, Security, and Breach Notification Rules.

In its announcement about this resolution with Health Fitness, OCR took the opportunity to outline steps healthcare providers, health plans, and business associates that are covered by HIPAA should take to mitigate or prevent cyber threats.

OCR noted that this settlement marked the fifth enforcement action in its Risk Analysis Initiative. That enforcement initiative was created to focus select investigations on compliance with the HIPAA Security Rule Risk Analysis provision, the foundation for effective cybersecurity and the protection of ePHI; to increase the number of completed Security Rule investigations involving potential violations of the Risk Analysis provision; and to highlight the critical need for organizations to prioritize compliance with this HIPAA Security Rule requirement. ●

CMA RECEIVES OFFER FROM VIFOR PHARMA

The UK's Competition and Markets Authority (CMA) has consulted on a £23m (\$29m) offer from Vifor Pharma in relation to the CMA's investigation into the company's conduct in the market for the supply of high-dose intravenous iron to the NHS. The offer is part of a wider set of commitments proposed by the company.

This is the first time a misleading claims case of this nature has been investigated by the CMA under its competition law enforcement powers.

The CMA's probe was in relation to whether Vifor Pharma had "restricted competition by making misleading claims to healthcare professionals about the safety and effectiveness of Monofer, a rival high-dose IV iron deficiency treatment supplied by Pharmacosmos."

The spread of disparaging misinformation is considered anti-competitive conduct, constituting a breach of competition law under Chapter II of the Competition Act 1998.

In addressing the competition concerns of the CMA, Vifor Pharma responded by offering commitments to:

- ◆ make an ex-gratia payment of £23m (\$29m) to the NHS;

- ◆ correct any potentially misleading communications disseminated by Vifor Pharma regarding the safety of Monofer and Ferinject, via a multi-channel

communications campaign to healthcare professionals;

- ◆ introduce several compliance measures to prevent the future dissemination of potentially misleading communications regarding the safety of Monofer and Ferinject to healthcare professionals.

A spokesperson for Vifor Pharma told GRIP: "CSL Vifor acknowledges the ongoing investigation by the CMA concerning the potential anti-competitive conduct of Vifor Pharma. After several months of detailed discussion, and as part of the CMA process, CSL Vifor has offered proposed commitments which are available on the CMA website.

"It is important to note that the commitments were offered without any admission of liability. We are pleased to be taking this important step towards resolution of the CMA investigation. However, as this is an ongoing investigation, we are not in a position to comment further at this time."

The CMA has taken on several cases in the pharmaceutical sector to protect and deliver significant savings for the NHS.

In total, it has imposed large fines of £400m (\$505m). ●

\$505m

Total fines from the CMA in the UK health sector

EU PHARMA LEGISLATION IN 2025 AND BEYOND

Key measures proposed as part of the EU's new pharmaceutical strategy include important changes to the procedures for the authorization and supervision of drugs, in response to concerns connected with patient access, antimicrobial resistance, environmental impact and innovation. An act addressing potential shortages of critical medicines aims to strengthen drug manufacturing capacity within the EU and reduce EU dependencies on other countries by way of a diversification of supply chains. There's also a proposed overhaul of the Supplementary Protection Certificate (SPC) system governing drug patent protection.

Negotiations on the package of measures continue. It is unclear whether an agreement can be reached in 2025 as key stumbling blocks remain. The most contentious issues relate to two contrasting objectives: incentivizing R&D through robust IP protection and market access for generic drugs within the bloc. Developments need to be closely monitored as they would almost certainly have an impact on drugs that are currently being developed.

JEFF LEMAY

Experienced Chief Compliance Officer **Jeff Lemay** reflects on his time at Jazz Pharmaceuticals and assesses the road ahead for compliance and legal teams across a sector that faces challenges ranging from regulatory upheaval to the arrival of new technologies.

JULIE DIMAURO

New market and policy initiatives in 2025 create a truly challenging healthcare environment, but they also present opportunities to expand into new areas, such as leveraging artificial intelligence (AI).

Functions are rarely siloed any longer, as teams collaborate to navigate ever-changing supply chain challenges, regulatory changes, data management and privacy concerns, and more.

My discussion with Jeff Lemay, recently Executive Director and Compliance and Ethics Officer at Jazz Pharmaceutical, formed the basis of a podcast discussion you can listen to on the GRIP website.

In our discussion, we spoke of regulatory change management, his expectations of regulatory changes on the horizon, supply chain and trade and tariff issues, drug approval timelines and risk, third-party risk management, and the fluctuating messaging around foreign bribery enforcement.

Lemay, who has experience working in both legal and compliance departments at businesses, has worked on the health policy side of the fence as well, and he can draw on a background in health economics. He remains optimistic about the state of compliance in this highly regulated business sector.

But there are challenges facing compliance professionals.

Regulatory change management

"This new era of the Trump administration and what it means for compliance professionals in the pharmaceutical industry will require ample dialogue between them and their leadership teams," Lemay said. "Although we're likely moving into a more



Regulatory
uncertainty brings
both risk and
opportunity to
pharma in 2025

risk-tolerant administration, the Office of the Inspector General is not going away, and that office's guidance and regulations cannot be ignored."

Lemay pointed out that the industry is working in a highly bipartisan environment when it comes to criticism of the pharmaceutical industry. President Trump has been silent about what direction he'll move in in the coming months and years.

"But if we look at how he responded in his prior administration, it was really around price negotiations. I anticipate more noise in this area, but where this will lead us is really a wait and see. So, we should remain vigilant and flexible in our approach."

FCPA uncertainty

I asked Lemay about areas where we might see more or less prosecutorial activity by the Department of Justice, and mentioned different messages the administration had put out (at the time of our discussion) in terms of enforcement, particularly in the area of the Foreign Corrupt Practices Act (FCPA). He said firms needed to be mindful of the fact that, just because the 1977 Act has been both narrowed down in scope

and stayed indefinitely as a law in the past couple of weeks, this does not mean their third-party risk management programs need to be altered.

The different messaging is confusing for compliance and legal teams, especially in such a highly regulated sector as healthcare where there are several enforcement cases on the books under that law.

"I don't necessarily think companies need to shift course in drafting additional policies or revamping them," Lemay said.

"I think what pharma companies should be doing is looking at this as an opportunity to really enforce the policies that they have for third-party risk. What I mean by that is that companies that can better manage risk, can better measure it, are in a better position to take on more risk."

Lemay sees it as a call to action for compliance functions to make sure they're keeping their policies front and center and that they're actually staying vigilant.

"I would not rush out and change anything. Just measure and manage the risk you have right now. In this environment – a more risk-tolerant one – that dialogue with your leadership needs to include the fact that they will likely see this as a chance to take on more risk.

"But in the compliance realm, we know risk is a pendulum. It could and likely will swing back," he said.

He explained that he meant the lighter touch by government agencies doesn't mean they were not watching and wouldn't be ready to strike when it was right. "They're still going to be enforcing the FCPA. But it's more of a wait-and-see position and a new prioritizing," he said.

Keep doubling down on third-party best practices, and if for some reason you don't



have them or find they are sub-par, build them up, he advised.

I mentioned the FCPA's five-year statute of limitations, which makes it likely to outlast the administration. Lemay agreed. "We need to stay true to the compliance procedures and practices that have proven effective for organizations and how they manage reputational and other risks," he said.

Communication strategies

While we work in a time of change, there are also some communications that need to be delivered to executive leadership and the board that outline strategies and bring a sense of reasoning and sensibility to what is going on in the environment, Lemay added.

"The board and its compliance committee, the executive leadership, they all hear the rumblings we do. We get different

slants to the same story, depending on the source. Some might believe the sky is falling, and it's incumbent on compliance professionals to sit back, absorb information and digest it to get a sense as to what it means for the business," he said.

Balancing act

Lemay used to work in a space that included rare disease research and treatment. Serious matters that can keep you up at night. But they don't have to, he said.

"We don't need to be paralyzed. We still have businesses to run, and this truly is a time when businesses in the US are taking on more risk," he said. That's OK, he reckons. But what we get paid for as compliance professionals is balancing different needs: the need of the business to make a profit; the business's future

direction; patients' needs (especially safety concerns); and the government's priorities.

Using AI

Technology enhancements are a big part of clinical trials today. Lemay emphasized that monitoring is essential for trials, but added the two main areas for tech deployment are pre-clinical and post-clinical trials, where there's a lot of opportunity.

"When you think about pre-clinical, that's drug discovery, and you can use AI in creative ways before using anything on a human. That's great information at a critical early stage. And post-clinical, you can use it for real-world evidence generation. Doing it faster and more efficiently," he said.

Although it doesn't mean these AI uses won't bring risk, it means there is less risk because we're doing them before or after humans are involved.

"When it comes to using AI in human trials, that's where I am a little nervous. I think AI could get there, but we're not there in this first generation of tools," Lemay said.

"My concern there is in how the Federal Drug Administration is going to use the AI outputs to validate the data you're looking at in a mid-stage human-based trial. We will likely get there, though," he added.

Gray areas are bread and butter

I asked Lemay in closing about his final thoughts for compliance officers in this industry sector at this time in our history.

"I think this is a really exciting time for compliance officers in the pharmaceutical space," he said. "And the reason for that is because if you're a compliance nerd like I am, this world of uncertainty and change is one that suits a compliance officer's strengths. We live in worlds of gray and rarely see things in black and white," he pointed out.

He said that a compliance officer's main job is not to say yes or no, it's to actually provide advice.

This is a great time to think about risk and get back to basics. "Do we have the proper policies to support the risk that we want to take? And, if not, it's time to revisit that. Those are the conversations you should be having with your boards and executive leadership. It might be a challenging time, but it's an exciting one," he said. ●

Jeff Lemay was speaking to Julie DiMauro as part of the GRIP podcast. Listen at grip.globalrelay.com

Lessons from McKinsey's OxyContin settlement

The matter-of-fact narrative is scathing about the moral and ethical void at Purdue as well as the behavior at the consulting firm.

THOMAS HYRKIEL
& JULIE DIMAURO



Consultancy firm McKinsey & Company was fined \$650m with a deferred prosecution agreement by the Department of Justice in December, for its role in the US opioid crisis.

The fine was levied as part of a criminal and civil settlement between the consulting firm and the DOJ in relation to the firm's work with Purdue Pharma from 2004 to 2019 on the marketing and sale of Oxycontin, an opioid painkiller with highly addictive properties.

Conspiring to misbrand

McKinsey faced charges of conspiring to misbrand a drug and obstruct justice.

A statement from McKinsey, posted prominently on its website, makes for fascinating reading.

It lays bare the frequently noted moral and ethical void on the part of the family members controlling Purdue, but is also a damning indictment of the culture at the consulting firm itself. It illustrates the dangers of presenting clever and hard-working people with work assignments that are unmoored from the human consequences resulting from their actions and the solutions that they devise.

This case has been written about and analyzed at length and there is already some excellent and exhaustive commentary.

Records destroyed

However, worth noting by specialist compliance and surveillance readers in particular is that one of the felony charges related to McKinsey "knowingly destroying records, documents and tangible objects with the intent to impede, obstruct, and influence the investigation."

Section XVII (pages 59 to 64) of the statement outlined the actions of McKinsey partners that led to this felony charge.

It demonstrated not only the awareness by the partners and staff of the fact that the consulting work they were doing was potentially untenable, but also a clear understanding of the importance of reducing or eliminating records in order to potentially avoid responsibility and accountability.

In this context, the messages between the McKinsey employees and partners involved are an instructive case study. They include the exchanges and actions that are shown in the box on this page. The Outlook event log clearly showed that

the deletion was not the partners' "typical practice." It appears that investigators were not able to subsequently retrieve the deleted documents and related off-channel communications.

This would certainly have at the least colored the DOJ's view of the firm and its culture and, possibly, had some impact on the size of the settlement.

It is a cautionary tale that highlights the need for an awareness of what channels are being used for business communications and the need for a policy and alert system that triggers an early warning when those channels are being circumvented.

To be sure, the company created a document titled *How We Have Changed* in December that outlined the significant changes it had made since 2019 to its technology, risk management policies, internal controls, Code of Conduct, training programs, and staffing resources in order to make the operational and cultural corrections needed to avoid further violations and reputational damage.

Along with the statement outlined above, this external-facing document could serve as a blueprint of action for other firms, as it is intended to hold McKinsey to the high standards clearly outlined in it. ●

iMessage exchange about emailing "opioid decks" to Purdue Pharma executives [Partner 3 and Consultant 6]

Partner 3: "what's bad in that deck..."

Consultant 6: "Nothin [sic] bad. We said we wouldn't do it. And creates a trail to the inline discussion. These guys will be deposed. Best our emails are not sucked into it."

Text message about OxyContin sales force reduction [Consultant 6 and another McKinsey Partner]

Consultant 6: "Don't want to create an email trail but the board decided to pull all reps from OxyContin."

Private / work email exchange [Partner 2 and Partner 3] Exchange between two work email addresses.

Partner 2: "Hope you're well. Can you send me your private email address. Want to send you a note."

Partner 3: reverted with private email address.

Follow on message to this private email address:

Partner 2: "Just saw in the *FT* that [a Purdue Pharma board member] is being sued by states attorneys general for her role on the [Purdue Pharma] Board. It probably makes sense to have a quick conversation with the risk committee to see if we should be doing anything other than [sic] eliminating all our documents and emails. Suspect not but as things get tougher there someone might turn to us." [Emphasis added in statement]

Response to message above from Gmail address:

Partner 3: "Thanks for the heads up. Will do."

Email to self [Partner 2]

Subject line: When Home Item listed: "delete old pur [Purdue Pharma] documents from laptop[.]"

Email to self [Partner 2]

"Remove Purdue folder from Garbage"

Action [Partner 2]

Purdue Pharma folder removed containing more than 100 items "many of which appear to be dated in critical timeframes" and seven of which "include the name of the Purdue Pharma CEO".



Risk as a catalyst for innovation

PwC's **Tiffany Gallagher** says use of new technologies is transforming the role of compliance in pharma organizations from a cost center to a strategic growth enabler.

ALEXANDER
BARZACANOS

In recent years, technological solutions have revolutionized compliance in the healthcare and life sciences industries. Once seen as an onerous cost center, compliance technology solutions are now being integrated across divisions to serve as a potent business facilitator.

One person who has witnessed this transformation up close is Tiffany Gallagher, US Health Industries Risk & Regulatory Leader at PwC. She said the sector is using emerging tools to make compliance programs more efficient and proactive.

But as technology becomes more efficient and complex, so would the regulators' expectations, Gallagher added.

New technologies

Gallagher said that pharmaceutical and medical technology companies were shifting compliance from a reactive cost center to a strategic business enabler by embracing advanced technologies and innovative operating models.

This transformation was, she said, enhancing risk management, driving operational efficiency and helping firms to embed compliance into the core of business strategy.

Digital tools, automation and data analytics were also enabling compliance teams to anticipate and mitigate risks earlier in the process.

"Predictive analytics support smarter decision-making, while automation reduces manual work and errors – freeing up resources for higher-value strategic initiatives," she told us.

Outsourcing and collaboration

"Innovative operating models, including outsourcing and agile frameworks, are helping organizations respond faster to regulatory change and scale their compliance functions more effectively. Cross-functional collaboration is also breaking down silos and embedding compliance across all areas of the business," Gallagher noted.

These advancements are delivering real results, such as improved regulatory readiness, with the ability to adapt to global requirements in real time. They are also helping to build stronger organizational resilience, particularly during market and regulatory disruptions.

A further benefit for Gallagher was the increased trust from stakeholders and regulators, which she said helped



Technology is shifting compliance from being manual and reactive to being automated, integrated and strategic”

differentiate firms in a crowded market. By integrating technology and new models, companies were positioning compliance to support long-term growth, innovation and competitive advantage.

“As compliance grows more complex, companies are outsourcing operationally intensive areas such as global spend transparency, healthcare professional (HCP) engagement management, monitoring and analytics, investigations and risk assessments. These areas demand precision, scale and specialized expertise, making them ideal candidates for outsourcing.

“Outsourcing also enables organizations to reduce workload, manage global regulatory complexity, and access new tools and talent without the overhead,” she stated.

She cited the example of transparency reporting benefits from AI-enabled data validation, expert reviews and automated audit-ready reporting across jurisdictions.

At the same time, monitoring and analytics deliver proactive insights through AI-powered transaction analysis, helping teams act before issues escalate.

But Gallagher also highlighted strategic benefits, including regulatory confidence, with continuous oversight and access to expert knowledge; operational efficiency, through standardized processes and automation; and cost control, with firms able to avoid the need for large in-house teams or legacy systems.

“Looking ahead,” she added, “companies are adopting hybrid models; keeping high-risk areas in-house while outsourcing execution. This enhances compliance effectiveness while allowing internal teams to focus on strategy and oversight.”

From data silos to automation

“Technology is central to modernizing compliance,” said Gallagher. “It is shifting the function from being manual and reactive to being automated, integrated and strategic. Legacy compliance systems relied on fragmented workflows, manual approvals and data silos, resulting in inefficiencies and increased risk.”

Automation, cloud platforms and real-time data are streamlining compliance. “These tools reduce administrative burdens, enhance audit readiness and lower the risk of human error. With structured digital records, organizations can respond faster to regulatory inquiries and scale compliance efforts more cost-effectively,” Gallagher said.

“AI and machine learning are elevating risk management by enabling predictive insights and smarter decision-making. Risk models evolve based on real-time data, helping teams detect issues earlier and tailor interventions before problems escalate,” she added.

Integrated compliance platforms also eliminate redundant approvals and disjointed communications, creating seamless, user-friendly workflows that improve internal efficiency and external stakeholder experience.

“Compliance is no longer a regulatory checkbox – it’s a source of insight, agility and value. Technology allows teams to shift from transactional to strategic, advisory roles. They’re helping the business innovate and comply,” she noted.

Changing compliance roles

“To fully leverage these tools, compliance professionals are developing new skills in data analytics, AI governance and digital operations. Organizations are investing in upskilling programs to help teams extract value from technology and lead transformation efforts,” she said.

“Regulators are raising the bar, expecting companies to adopt advanced technologies to manage risk more effectively. Compliance teams must demonstrate they can proactively identify and mitigate risks – using the tools available to them – to meet heightened expectations.”

By embracing this shift, compliance functions can move from reactive oversight to business enablement, contributing to resilience, innovation, and long-term value.

Managing third-party risk

“Managing third-party risk is a growing priority as companies expand global

networks and face increasing scrutiny,” Gallagher said. “To keep pace, organizations are combining technology with external expertise to build more scalable, proactive risk management programs.”

Automation and embedded controls are streamlining third-party due diligence, while AI and advanced analytics enable real-time risk monitoring and trend detection. This allows firms to focus on high-priority issues and reduce manual oversight burdens.

And external partners bring market intelligence, regulatory updates, and benchmarking data that strengthen audits, enhance risk scoring and improve oversight of vendors and distributors.

“Together, these capabilities support more agile, data-driven third-party risk management. Companies can continuously assess, monitor and respond to evolving risks. This improves compliance outcomes, strengthens stakeholder confidence and maintains operational integrity across complex supply chains,” she stated.

Changes to risk management

“In response to rising complexity, companies are adopting a more dynamic, integrated approach to risk. There’s a shift from risk avoidance to risk agility – viewing risk not as a constraint, but as a catalyst for innovation when managed proactively,” said Gallagher.

Real-time risk sensing, scenario modeling, and AI-driven dashboards are replacing static assessments. Cross-functional teams – spanning compliance, legal, supply chain and IT – are working together to monitor risks continuously and respond to issues in real time.

“Enterprise risk functions are becoming more unified, supported by shared data, common taxonomies and enterprise GRC platforms that span functions and geographies. Environmental, social, and governance (ESG) issues and cybersecurity matters are core to the risk framework, particularly given the rise of digital health and AI-driven R&D,” Gallagher stated.

There’s also a move toward outcome-focused risk strategies – where success is measured not based on the number of controls in place, but rather on the speed and effectiveness of risk response, impact on patient safety, and alignment with innovation goals.

“Companies that embrace this transformation are better positioned to navigate uncertainty, seize opportunity and build resilient, future-ready organizations,” she added. ●



Risk domains are constantly in flux.
But right now, the big three in third-party
management are anti-bribery and corruption,
cybersecurity, and human rights”

DENIS JACOB

Denis Jacob, Ethics and Compliance Business Partner at global medical equipment manufacturer Henry Schein, explains why the current environment means compliance professionals need to think differently about risk.

JULIE DIMAURO

In the high-stakes world of healthcare compliance, managing third-party risk requires more than a regulatory checklist – it demands a nuanced, strategic approach.

Few people understand this fact better than Denis Jacob, Ethics and Compliance Business Partner at global medical equipment manufacturer Henry Schein. With over two decades of experience spanning compliance, risk management, and internal audit, Jacob has navigated the evolving complexities of third-party oversight in medical and pharmaceutical markets ranging from his native Latin America, to the US, and well beyond.

“My experience is global. I’m originally from Brazil and did a lot of work in Latin

America but have been living in the US for about a decade now. I work with global organizations and manage teams all the way from Mexico to Australia and all the countries in between,” he explained.

He added that while global in geography, his experience had been more or less exclusively focused in and around healthcare, whether in the medical device sector or pharmaceuticals.

Jacob joined us on the GRIP Podcast recently to talk about a host of issues. We discussed the major risks facing healthcare companies today, how these organizations can improve their risk management frameworks, and why all compliance professionals need to think more like business strategists than regulators.

A shifting risk landscape

“Risk domains are constantly in flux,” he explained. “But right now, the big three in third-party management are anti-bribery and corruption, cybersecurity, and human rights – particularly forced labor. Each presents unique challenges, but they’re interconnected in ways that companies often fail to recognize.”

The challenge, Jacob noted, is that businesses have traditionally addressed these risks in silos. In the past this has often led to inefficiencies and may even have contributed to compliance failures.

“Fifteen years ago, when the Foreign Corrupt Practices Act (FCPA) enforcement wave hit, compliance teams scrambled to build anti-bribery programs. Now,



cybersecurity has taken center stage, often managed separately by IT or security teams. Meanwhile, human rights concerns – driven by new regulations on forced labor – are frequently handled within procurement.”

The result of all three developments is that there is a completely fragmented approach to risk and compliance that burdens third-party partners with redundant requests and leaves major gaps.

But fixing this issue doesn't need to be complicated. With a refreshing simplicity, Jacob proposed a solution that makes sense regardless of sector.

“Companies need to integrate their risk assessments,” he said. “A holistic approach not only makes compliance more effective,

but also eases the process for third parties, ensuring better cooperation and more accurate data.”

Beyond the checklist

Jacob said there had been a major and fundamental shift in how companies should approach third-party oversight. “For too long, compliance has been about issuing endless questionnaires, ticking boxes, and performing audits. That doesn't cut it anymore.”

Instead, he advocated for a more nuanced model, where compliance professionals learned about and deeply understood business operations. This would mean they are therefore able to tailor oversight actions accordingly.

“Take supply chain disruptions, which is something the pandemic exposed in brutal detail. Compliance officers are now working far more closely with their partners in the procurement teams, because they need to understand not just who their third parties are but who, in turn, those third parties might rely on.”

He cited the risk of human rights and labor abuses as a good example of how such a deeper level of due diligence was developing a rising awareness of potential flaws in the behavior of suppliers.

“You may think that you know your supplier well, but how much visibility do you really have into their suppliers? And in simple terms it is no longer acceptable for companies to claim ignorance. »



Compliance isn't just about avoiding risk.
It's about enabling sustainable,
long-term success"

Regulators, consumers, and investors expect transparency, and companies that fall short face serious reputational and legal consequences."

Moreover, Jacob noted that third-party relationships can often evolve over time, as a contract develops in often unexpected ways. "A supplier hired for one function might later take on additional roles, which can introduce new risks."

His solution was to suggest that the vetting process is not just a once and done affair. "Continuous monitoring – not just initial vetting – is crucial to managing these shifts effectively," he said.

Companies must also consider the geopolitical and regulatory landscape when managing third-party risks. At a time when the new US administration is forcing a rethink on the rule book on global trade and the former consensus looks more uncertain than ever, he suggested including trade and supply chain issues as part of any evaluation of risks.

"Sanctions, tariffs, and trade restrictions can suddenly change the viability of a partnership. Businesses need mechanisms in place to monitor these changes in real-time and adjust their strategies accordingly."

The unsolved challenge

Among the many emerging risks, Jacob ranked cybersecurity as one of the most pressing and urgent.

"In healthcare, data is everything," he explained. "We're dealing with critical patient information, connected medical devices, and vast digital networks."

This fundamentally more connected world means "a single vulnerability can bring down an entire system."

He pointed to the FDA's recent push for stronger cybersecurity measures in medical devices. "It's no longer just about compliance; it's about patient safety," he pointed out.

"If a connected device gets hacked, it's not just a data breach – it's a potentially life-threatening situation. Companies must take a lifecycle approach to security, ensuring products remain protected long after they hit the market."

Beyond medical devices, Jacob highlighted the growing role of cloud computing and third-party software solutions in healthcare. "Many organizations rely on external vendors for data storage and analytics, which creates additional exposure. Strong vendor risk management is critical to ensuring security across the entire digital ecosystem."

Jacob emphasized the importance of continuous testing and updates. "Cyber threats are evolving constantly, so your defenses must evolve, too. Companies should conduct regular penetration testing, ensure their software is updated, and require their third-party vendors to meet the same security standards."

Compliance officers as strategists

For compliance professionals, Jacob emphasized the importance of shifting from a reactive, rule-enforcing role to a proactive, business-minded approach. "Too often, compliance is seen as an obstacle to business rather than a partner. That needs to change."

And his advice to his fellow compliance officers, in healthcare but also in other regulated sectors, was to do all you could to learn what makes your business tick.

"Know your business inside and out. Listen to earnings calls. Understand your company's strategic goals. If you don't, you'll always be playing catch-up when new risks emerge."

For Jacob this mindset shift is at the heart of how compliance teams need to act and it extends to how those teams interact with employees in other parts of the business.

"Training can't just be about reciting laws and policies. It needs to be role-specific and practical. Sales teams, for instance, should understand third-party risk not in legal jargon, but in terms of contract negotiations, pricing structures, and red flags they might encounter in daily interactions."

As Jacob sees it, compliance teams should have clear cultural objectives. "The goal is to build a culture where employees recognize potential risks on their own and feel comfortable raising concerns."



For Jacob, this need for compliance to be deeply embedded in the business runs both ways. Compliance needs to be embedded in strategy from the start, but strategy teams also need to take a compliance-first approach. As he summed it up: “Compliance professionals should be part of strategic planning discussions, not just called in after decisions are made. That’s how you prevent risks instead of just reacting to them.”

AI is a powerful but risky tool

There are few areas of business not currently looking at how best to adapt to and adopt artificial intelligence. Healthcare compliance is no exception. Jacob acknowledged the excitement around AI but warned against adopting it blindly. “AI

is an incredible tool, but it’s not a magic fix. If your underlying data is flawed, AI will only amplify those issues.”

Here, as elsewhere, his focus is on the need for strong governance. “Companies need clear policies on AI use, robust data management practices, and human oversight to ensure AI-driven decisions don’t introduce new risks. Otherwise, you’re just automating bad processes.”

Jacob also highlighted AI’s potential role in compliance monitoring. “AI-driven analytics can help identify anomalies in financial transactions, supply chain data, and vendor interactions. But without proper oversight, it can also generate false positives – or worse, miss critical red flags.”

Organizations must also consider ethical implications. “Bias in AI models is

a major risk. If the training data is skewed or incomplete, AI-generated insights can reinforce existing biases rather than mitigate them. That’s why human oversight remains critical.”

Resilience through better planning

Jacob was clear that all these many potential disruptions and distortions pointed in the same way. Climate-related disruptions, geopolitical instability, and supply chain vulnerabilities all point to one critical need: business continuity planning.

“Companies can’t just assume things will go as planned,” he said. “They need to pressure-test their operations. If a key supplier goes down, can you pivot quickly? If a hurricane wipes out a manufacturing site, is there a backup plan? These aren’t theoretical risks – they’re happening now.”

Jacob underscored the importance of treating business continuity as an ongoing strategy rather than an annual exercise. He sees it as a process more than an event.

“It’s not just about having a plan on paper. It’s about actively testing that plan under real-world conditions. The companies that survive disruptions are the ones that plan for them.”

He also stressed the importance of communication and coordination. “A business continuity plan is only as good as the people executing it. Employees must know their roles, and companies must ensure smooth coordination between departments and external partners.”

The appliance of compliance

Asked about the most rewarding aspect of his career, Jacob reflected on the impact of compliance done right. “The best moments are when you see the business thrive while doing things the right way. I’ve seen companies avoid massive scandals simply because they took the time to select ethical partners and implement strong controls.”

For compliance professionals looking to make a real difference, he offered one final piece of advice: “Compliance isn’t just about avoiding risk. It’s about enabling sustainable, long-term success. If you approach your role with that mindset, you won’t just be a compliance officer – you’ll be a strategic leader.” ●

This is an edited transcript of a GRIP Podcast in which Denis Jacob was interviewed by Julie DiMauro. To listen to this and all previous episodes, visit grip.globalrelay.com



India must regulate to safeguard its reputation as “the world’s pharmacy”

Despite well-established manufacturing infrastructure, India is facing a challenge to maintain its market dominance, as China waits in the wings.

HAMEED SHUJA

For decades, India has taken pride in its status as the world’s largest producer and exporter of generic drugs. It also has one of the world’s largest pharmaceutical industries.

Last year, the annual turnover of India’s pharmaceutical market was estimated at \$65 billion. According to other estimates, that figure will reach \$130 billion by 2030. And by 2047 it could have sky-rocketed to \$450 billion. Its vast manufacturing

infrastructure has long enjoyed the trust of the world’s toughest drugs regulators, including the US Food and Drug Administration (FDA).

Other factors have also worked in India’s favor recently. The West, especially the US, is trying hard to decrease reliance on China for drugs used in clinical trials and early-stage manufacturing. India provides a natural alternative. The US is India’s biggest foreign partner in the pharma sector. Four out of 10 prescriptions filled in the US in

2022 were provided by Indian companies. They also provided 47% of all generic drugs prescribed in the US that year.

The availability and provision of affordable life-saving Indian medicine to US citizens also saved the US healthcare system some \$219 billion in the same year.

So, it’s not just about pride. It’s also profit. But maintaining profits requires a healthy reputation, among other things. And that’s what is under threat, as is India’s status as “the world’s pharmacy.”

Regulators in India need to resolve a number of key challenges, both at home and abroad, to safeguard the country's position and reputation in the global pharmaceutical industry.

Regulation

Regulatory failures at home, as well as criticism from regulators abroad, have hindered India's ambitions to cement itself as a global pharma powerhouse.

Last August, the country's Central Drugs Standard Control Organisation (CDSCO) accepted in a report that around 50 drugs produced in the country were "not of standard quality." They included commonly used names such as paracetamol, amoxicillin and vitamin B supplements.

A source at the regulatory body told *Business Standard*: "The drug regulator constantly monitors drugs and samples are randomly tested every month to ensure their quality as well as safety standards."

The source insisted prompt action was taken against firms responsible for manufacturing sub-standard drugs. But the damage was done and the story raised eyebrows and made headlines globally.

The CDSCO and India's other regional drug regulators have also failed to prevent the production of counterfeit drugs across the country, prompting critics to call India's overall drug regulatory system 'a massive failure.'

In the most regrettable incidents, a number of child deaths in The Gambia, Uzbekistan and India in recent years were linked to the use of toxic cough syrups manufactured in India. Regulators eventually banned the medication in 2023.

Indian parliament

In March this year, an Indian parliamentary committee warned the same regulator to put its house in order and resolve ongoing issues and failures, following concerns that the world's largest generic drugs producer was losing ground to other regional rivals.

The Parliamentary Standing Committee on Health and Family Welfare accused CDSCO of unnecessary delays, a lack of transparency and centralization of authority around issuing licenses to medical devices, prompting manufacturers to move to Vietnam and Malaysia instead.

Criticism has also come from foreign regulators. For example, the FDA has sent warning letters to Indian-based manufacturing firms for "violations of Current Good Manufacturing Practice



It's about marketing India as a country. We need to show we consistently meet high standards. Big pharma is hesitant to risk high-value raw materials"

(CGMP) regulations for finished pharmaceuticals."

Despite the US being India's largest trading partner of generic drugs, the US drugs regulator has repeatedly criticized India's manufacturing processes and standards and described them as falling short of US and other global requirements.

European regulators have also suspended hundreds of Indian-made drugs in the past due to unreliable tests conducted by Indian partners and manufacturers.

Production

China won't just sit back and let India take over. Certain practices in recent years indicate a desire to undermine India's capacity to produce high-quality medicine for global markets.

For example, Indian regulators have been criticized for failing to prevent China's dumping of non-pharma grade ingredients, such as IPA (iso-propyl alcohol) into the Indian market.

This has undermined global trust in India's pharmaceutical industrial standards. Countries including the US are concerned about Indian drugs being diluted with low quality Chinese ingredients.

India's pharmaceutical sector itself relies heavily on Chinese stocks of key starting materials (KSM), or the basic ingredients used in the production of generic medicine. According to studies, China provides around 40% of the global demand for KSMs. This over-reliance and lack of diversification has left both India and the US concerned.

And there are also questions around reliability. Experts believe the country has failed to convince international investors that they can trust its manufacturing

capacity with high-value raw ingredients and still get strong results.

According to Rhonda Duffy, chief operations officer at Biocon Biologics: "It's about marketing ourselves as a country. We need to show that we can consistently meet high standards [...] Big pharma companies are hesitant to risk high-value raw materials here, unless we can guarantee reliability."

Way forward

India has the ambition and the capacity to become a \$10 trillion dollar economy by the year 2032. And the pharmaceutical industry is set to play a major part in helping the country reach that goal.

To do this, the industry has to overcome a number of key challenges, mostly to do with production and regulation at home, but also with safeguarding its reputation and status abroad.

For a start, it has to work for self-sufficiency in relation to KSMs and other key ingredients required for the production of generic drugs. Over-reliance on China doesn't help India's ambitions in the pharma sector. In fact such a reliance, if anything, undermines them.

Second, India needs to get serious about regulation. As experts have suggested, strong enforcement action should be a rule, not an exception, when it comes to dealing with regulatory violations.

This is vital because, as discussed above, failure in this area can cost lives around the world. It can also cost India its status as the largest source of affordable life-saving drugs for the rest of the world.

Third, India needs to find a way of 'working with' and not 'working separately' from European regulators. In the recent past, issues around the sharing of pharmaceutical and manufacturing data have caused tensions, both at business and political levels.

Such tensions don't serve Indian interests, and New Delhi has to move away from the 'my way or the highway' approach when dealing with foreign governments and regulators.

Lastly, India has to sort out its leadership problem. The government should not only do more to support both the industry and the regulators, it should actually take the lead.

Again, in the words of Duffy: "The smartest people I've ever worked with are in India, but the leadership skills – really poor. We need leaders who can inspire their teams, not just command them." ●



Compliant growth in biotech

Ravi Monangi and **Ethan Grammer** of Celito Tech discuss how smaller pharma and biotech firms can minimize compliance risk as they scale.

ALEXANDER
BARZACANOS

As costs mount in the pharmaceutical and life sciences industries, regulatory compliance can easily become seen as a mere nuisance for companies breaking into the industry.

But sidelining these functions early on can be a critical mistake. Failure to conduct early due diligence can lead to major setbacks at critical stages of a pharmaceutical company's development, from clinical trials to IPOs.

GRIP spoke with Ravi Monangi and Ethan Grammer, respectively Founder & CTO and Senior Manager, Strategic Cybersecurity & Infrastructure Initiatives, at Celito Tech, a firm providing strategic cybersecurity, compliance, and quality assurance functions to small and mid-sized biotech and life sciences companies.

Founded by veteran biotech IT leaders, Celito specializes in providing fractional services that might not be cost-efficient to conduct in-house.

Industry participants face major challenges, such as how to manage sensitive data transfers effectively, while bolstering cybersecurity protections. These issues are more salient than ever thanks to an emerging policy drive to reduce regulation, prevailing uncertainty surrounding biotech investment, and an increasing number of sophisticated cyber attacks.

How can firms uphold effective, cost-efficient standards that minimize risk and prevent early compliance mistakes in a company's growth cycle?

Managing the data continuum

Monangi and Grammer noted the complex challenge posed by keeping sensitive data safe as it is maintained and transferred between various institutions.

These create significant issues at the IPO stage, with the SEC becoming increasingly vigilant in ensuring companies accurately report cyber risks and security breaches.

"Sensitive data moves through a continuum of organizational systems, where it can be transformed. For example, if someone is participating in a clinical trial, they are likely to visit a hospital or doctor who either recommends or administers the trial medication," explained Monangi.

"From there, data is transferred from the point of care to outsourced research organizations hired to manage the trial. The sponsor company receives the data, which may include aggregated results, and then data is submitted to health authorities.



'Good' to auditors means you have a process that can be defined, documented and audited"

"In that continuum, companies might raise funds and become public companies. If there is any breach or security incident that triggers the SEC's security materiality requirement, they would have to deal with SEC reporting."

He added that when companies get to the commercial stage, they will usually be gathering even more protected health information from things such as adverse events, via patient services teams that are dealing with the patients directly, and from healthcare providers providing a patient's information to help the company do more research on whether their drug is having a potential issue.

"So, throughout the entire life cycle, there's a lot of points in time where the data needs to be secure," Monangi said.

Grammer added: "As part of the SEC 10-K filings that companies must submit, the cybersecurity section focuses on what the company's risks are, how the company evaluates risk, and what procedures and individuals they have in place, and whether they are insourced or outsourced."

And when companies do quarterly and annual auditing, there are sections dedicated to cybersecurity. "We saw at the end of 2023 that the SEC expanded those cybersecurity requirements to be more consistently reported than they were previously," said Grammer.

What are regulators looking for?

Asked what good looked like for regulators, Grammer said: "At a higher level, 'good' to auditors and authorities means you have a process that's defined, documented, and can be audited. Those are the three big areas. And that process, because so many of these companies work with third parties, needs to be documented from the

start of the relationship to the end, where both sides will have the ability to provide trails to the audits."

Monangi added that there should be no misrepresentation or fudging of information. "It matters that there is no fraud or waste in these processes. The FDA cares about whether there is any compromise on human safety. At the same time, regulators care if the company is making those health claims accurately.

"Regulators want to make sure about the chain of custody or the integrity of the data origin, the transformations it went through, the storage it went through, and what was submitted," he said.

Off-channel communications and decentralized policies

Monangi noted that life sciences industry participants often engage in off-channel communications and unintentional sharing of sensitive information. To counteract this, compliance teams need to be given visibility of these communications to make sure they adhere to regulatory requirements.

"Casual methods of transferring data are quite common, especially among early-stage companies. Firms go with simplistic approaches instead of creating policies that ensure the system's configuration is such that only the right people can access it. Celito works with companies to ensure that data is stored and transferred in a secure and compliant manner while maintaining cost-effectiveness," he said.

"From the DOJ's perspective, it is clear that off-channel communications, if they're a part of an organization's policies, must be archived and audited. In the life sciences area, we see this primarily when businesses reach that point of having a sales force where they're out knocking on the doors of healthcare providers. They are communicating a lot internally, but also externally. So, making sure that they're not transmitting protected health information in a way that isn't secure and isn't approved by the company is important."

He added that from the FDA's perspective and the HIPAA compliance perspective, it's important that internal compliance teams have visibility over what's happening in the organization, no matter the form of communication.

Monangi also noted a problem of decentralized internal policymaking, which can become increasingly problematic as the company grows. In early-stage companies, governance rules are not always centralized. »

Business teams often take control of the process and manage it in isolation. These siloed relationships within the organization mean there's a lack of standardization when it comes to gathering data from contract research organizations in a unified way and applying consistent security and privacy measures. This level of maturity typically doesn't emerge until later.

"We advise that it's much easier to implement good practices from the start. It's best to design security measures early rather than waiting until later, by assuming there won't be audits or that the odds of reaching phase three with their drug are low. Companies often think this way because they're focused on keeping costs down and simplifying processes, but this just ends up causing bottlenecks later," explained Monangi.

Managing third parties

Vendors can be a key point of risk for data security, and it is critical to manage them correctly, Monangi said. Vendors can create risks related to data accessibility and integrity, and maintaining explicit contractual agreements highlighting compliance standards is of critical importance.

"At times, companies need to enforce standards with vendors. This can be achieved by incorporating clear expectations into the service agreements. Vendors are typically prepared to meet these standards. They just need to be explicitly requested or included in the contract to ensure compliance. If you address these needs after the fact, you may face additional charges.

"We've seen cases where, once we get involved, companies reach out to vendors, only for vendors to claim it wasn't part of the original contract and demand higher fees. This makes it harder to justify the cost and navigate business use cases. By doing it right from the start, you can avoid these issues and keep costs manageable."

Monangi explained that early engagement allowed his firm to help design necessary policies and configurations for ingress and egress systems, ensuring a smoother, more cost-effective process.

Compliance with EU regulations

Monangi and Grammer noted that American biotech and pharmaceutical companies are turning an eye towards Europe, known for its strong privacy and data protection laws.

Getting ahead of managing patient data to make sure it is compatible with the EU

General Data Protection Regulation (GDPR) before deciding to enter the market is a prudent investment.

"In life sciences, companies are expanding clinical trials to Europe or globally. They might start in the US if it's a US-based company, but then expand the trial to European countries. That's where regulations such as the GDPR kick in," Monangi said.

Grammer added: "GDPR compliance services have become more and more popular as companies expand clinical trials to the EU more quickly than they have in the past. To [Monangi's] point earlier, they may start in the US for a phase one trial, but for phase two or later phases, they may be moving to the EU or to Australia or Japan, which have completely different privacy regulations around data. Those are some of the main trending questions that we're getting."

Monangi added: "That's where the informed consent forms are going to become important. Subject rights management is going to become important, data breach notifications: all these things will become relevant at that time."

Room for improvement

Monangi pointed out that the biotech sector is characterized by excessive physical documentation, which can slow down processes and inhibit technological advancement. Many companies are still heavily reliant on manual workflows, which can divert focus from security risks.

"This is inefficient," Monangi said, "which may be rendering firms less able to focus on risk because they are held up by document-centric workflows or human-centric workflows, which require a lot of manual

touch points. These methods are also not cost-effective. Change is happening, but it is very slow compared to other industries."

Deregulation and the future

While deregulation may be occurring, the threat landscape remains strong, particularly for data protection, Monangi said. But regulatory changes should be expected in emerging areas such as AI.

The COVID-19 pandemic accelerated the move towards decentralized clinical trials, and companies are designing trials with contingency plans to ensure resilience and continuity during disruptions, he added. Plus, companies should stay vigilant about protecting data from malicious actors.

"We might be seeing regulation loosening, but we're not seeing a drop in the number of adversaries that are wanting to take advantage of companies' data. That is a very real threat that still exists and is increasing. The need to protect intellectual property, patient data, internal employee data, will remain very real, regardless of whatever regulation exists in the industry.

"There has been a significant emergence of use cases, spanning from drug discovery, synthetic clinical trials, digital twins, agent therapy, and software as a medical device. While there are guidelines from health authorities, true regulations haven't fully evolved yet.

"I was reviewing an article that highlighted the exponential growth in AI-enabled clinical trials, with a sharp increase in submissions from 2019 to now. The industry is actively leveraging cutting-edge technologies, and in this context, transparency is key," said Monangi.

As an example, he pointed to how firms wanted to tap into wearables and sensors to be able to run trials more efficiently through decentralization. "For a clinical trial, a patient can go to the nearest lab, or they may wear a device and communicate outcomes. But these processes haven't reached a stage where they are fully regulated. The US created a draft guidance based on Europe's AI Act, but more is still yet to come," Monangi said.

Grammer added: "In the financial sector, for example, we've seen firms hit with large fines because they didn't protect or audit their generative AI use. It's feasible to think that we may see the same thing in the life sciences industry in time, just as a result of the fact it's becoming more and more desirable for firms to use all these cutting-edge technologies." ●



It's much easier to implement good practices from the start. It's best to design security measures early, rather than waiting until later"

Grip.

GRIP is your essential source of expert insight, regulatory updates, and practical guidance •

- Stay abreast of changes in compliance, regulation and technology with daily expert analysis and real-world intelligence at your fingertips.
- News, insights and so much more.
- Our talented team of experienced journalists, lawyers and regulatory experts ensures that accurate and up-to-date information reaches you when and how you want it.
- Find GRIP at: www.grip.globalrelay.com

Weekly Podcasts

Our expert-led podcasts offer practical insights and advice on the latest regulatory trends.

Rules Navigator

Save time and reduce risk with a tool that offers plain English summaries of key rules and regulations.

Country Guides

Our comprehensive country guides feature intel on local compliance, data and technology laws and enforcement decisions.

Meet our expert team

Made up of industry experts with extensive knowledge of finance, compliance, and regulation our team will help you navigate regulatory challenges with confidence.



Alexander Barzacanos
Deputy Content Manager
and Editor



Martin Cloake
Managing Editor



Carmen Cracknell
Senior Reporter



Julie DiMauro
US Content Manager



Viada Gurvich
Senior Reporter



Jean Hurley
Commissioning Editor



Thomas Hyrkiel
Director, Content and
Community



Martina Lindberg
Production Manager



Rob Mason
Director, Regulatory
Intelligence



Hameed Shuja
Senior Reporter



Alex Viall
Chief Strategy Officer



AARON NARVA

Conflicts of interest are everywhere in healthcare. **Aaron Narva**, Founder and CEO of Confluxis, explains how his technology is helping organizations use the huge quantities of data in the industry to look for patterns and spot any irregularities that may need investigation.

JULIE DIMAURO



Humans are being digitized through new devices, apps and monitoring technologies, which are tracking, analyzing and storing a massive amount of data.

This data, and how people interact with it, can create conflicts of interest. And this is, arguably, more relevant in the healthcare sector than in any other. Approximately 30% of the world's data volume is being generated by the healthcare industry. The compound annual growth rate of data for healthcare is set to reach 36%. That's 6% faster than manufacturing, 10% faster than financial services, and 11% faster than media and entertainment.

Aaron Narva, the CEO and Founder of Confixis, a technology firm that helps businesses identify, investigate and manage conflicts of interest within their organizations, spoke to GRIP about sorting through this data to minimize risk.

Narva's background makes him well-placed for embarking on this type of business enterprise; he was a white-collar crime investigator who in that capacity has worked on everything from money laundering issues to foreign corruption issues to construction fraud.

"Analysis of conflicts is about taking an old process, that is basically the collection of data from healthcare providers as a check-the-box exercise, into a data collection and analysis exercise that drives better decision making in healthcare organizations. Put simply, that means better decision making around legal risk, regulatory risk, but also research integrity risk," Narva explained.

The technology solution offered by Narva digs down into where large healthcare organizations spend their money and why they spend it on the things that they do. He said healthcare is the only industry where you can see, in a granular way, the choices that people make every day in their jobs – and with data.

"That's very difficult to see in other places. It exists in finance to some extent, but in healthcare you can see it. And the financial incentives in healthcare often run at crossways to each other," he said.

Prevalent conflicts

Associations like those in consulting relationships are commonplace. Things we can see publicly are most readily observable, such as what pharmaceutical

and device companies are paying to doctors. But there are certainly payments for services other than consulting. Physicians could have outside financial interests. For example, if a physician owns a piece of real estate, and there's a clinic on that real estate, and then the physician refers patients to that clinic, and also charges below market rent for that real estate ... well, that could be seen as a kickback, he explained.

To some extent, the American fee-for-service model is almost what you could call a conflict with someone's health, because the incentive in that model is to build more products and not necessarily to think of the patient's health first, Narva said.

"I think our goal as a company is to say, OK, conflicts appear to be everywhere, but let's analyze the data. Let's analyze people's decisions and help people figure out where it looks like a conflict – but may or may not be one," he said. "Let's find the true conflict and determine the mitigating actions that can be taken to protect the provider, to protect the healthcare organization, to protect the pharma company, to protect the payer, whoever it is that's involved.

"Our health system is built around one big conflict of interest. What incentive do these professionals have in totally curing me or totally curing all people like me with that condition?"

Narva's view is that, at least in the public healthcare sector, there are great restrictions on people's ability to have outside business activities. That can help. But, he pointed out, there's still that inherent conflict within healthcare in terms of what you're trying to solve, and where your interests lie.

"As long as people are making incremental money based on incremental

procedures and prescriptions, there's always going to be a conflict.

"We're not conspiracy theorists, we're not in that business," Narva emphasized. "In fact, we try to be judicious. But that's the thing that's interesting about a conflict. If you don't have contextual information – which we really don't often have – you have to get that directly from the parties. We often just see a payment or another action done," Narva explained.

"I think governments and regulators and the public and payers and healthcare systems in general are starting to look at all these conflicts and say, in the absence of contextual information, where do we need to go and get that information to say, 'yes, this was fine. This is not a big deal and there's a reason for this money.'

"We feel truly that collaboration between industry and providers is really important to have better technology to create better therapies, to do better things," he said.

Healthcare provider organizations and hospitals are spending a lot of money potentially as a result of conflicts of interest, Narva said, emphasizing that the conflict is leading to additional spend. This is one of the reasons why companies care about unearthing and solving for them – beyond the rules and laws about them.

Patient trust

Asked about research bias, referral patterns, and patient perception, Narva agreed that even if a conflict of interest is not actively influencing healthcare providers' decisions, the perception of a conflict could erode patient trust. "There are many examples of this. Even in institutions where maybe no one broke the rules per se, or a relationship was even properly disclosed, just the fact that the



Our goal as a company is to accept that conflicts exist, but to find the true conflicts and to figure out mitigating actions that can be taken to protect whoever it is that's involved”

»

relationship exists was enough to create a problem,” he said. “I think the erosion of trust is a major issue.”

The CDC just released its conflicts of interest reports for its vaccine committee, Narva said. The members disclosed the conflicts. And if anyone had a conflict, they didn’t vote on that issue. That’s exactly how it’s supposed to work.

“That is when the conflict mechanism has done its job, which is to say that those people who had a financial interest in something happening just recused themselves and didn’t vote on that matter. But simply disclosing a conflict [as per regulatory requirements] doesn’t do very much in and of itself. It’s not a curative thing,” he observed.

Question of trust

Speaking of trust, Narva mentioned how trust in healthcare before COVID was at roughly 71%, but it has dropped to 40%.

“That’s a massive erosion in trust. Institutional trust in general is going down, but when people find out that doctors have financial incentives to make a decision about their health, that really creates a problem,” he said.

“We can talk about research bias, but it’s not just that someone has a stake in the outcome when they are doing research for a company they own stock in. That’s pretty rare.

“But someone could be a spokesperson, promoting a company’s drugs or devices, receiving money to learn all about a company’s drugs and devices in a way that’s not educational necessarily. How can that person be doing unbiased research for that company? Well, the answer is they could,” Narva said.

Consumer demand

Without some insight or contextual understanding of those other relationships, we will never know, he said.

“People are afraid to talk about this out in the open because it’s sort of just how business gets done. But consumers are going to be demanding more of this information and they want to better understand it,” he said. And that means there will be a lot more accountability around it.

For businesses, really, this is fine, because some decent percentage of these things turn out to be OK anyway, he said. Figuring out what is truly an issue is critical.

Narva talked through what his



We look for behavioral patterns and outliers – signals in the data that tell us that something unusual is happening. It doesn’t mean something bad is actually happening though”

technology does. “We take data, different kinds of data, like provider self-disclosed data, which is usually mandated in health systems. We take health system data about where they spend their money and about outside relationships. And we look at public records data relating to relationships. And we do some proprietary stuff in terms of pulling data out of the public record. And we buy a bunch of data, too.

“So we buy data from different places. Then we match all that stuff together and look for patterns,” Narva explained.

Since a decent amount of enforcement is driven by whistleblowers, it’s often the perception that matters more at the end of the day, he said.

“We look for behavioral patterns and outliers – signals in the data that tell us that something unusual is happening. It doesn’t mean something bad is actually happening, and we would never go to a client and say, ‘here’s a conflict

of interest.’ That’s not how this works,” Narva said.

“And we typically don’t use that terminology when interacting with our clients. We say, ‘here’s risk, and now let’s think about how you mitigate this risk.’

“You can look at the risks that come along with dealing with a supplier. What are the reasons that you’ve chosen that supplier – and are they the ones that are best for the health system or not. Are they the ones that are best for somebody else?”

“We look for the areas of influence inside organizations to make certain decisions – pulling out the patterns to help people better understand the dollar impact and the risk impact of each decision that’s being made so that they can decide what they want to address,” Narva said.

This analysis of one’s own data is essential, Narva said, because you’re on the hook for data you’ve collected. His best tip for those who own data is to be

hard on themselves and ask themselves tough questions.

"Look at it the way a regulator or a payer or an investigative journalist would expect you to," he explained.

Stakeholders want this intelligence

Narva said that at the very beginning, he and his team were mostly interacting with compliance, but that has changed. "There are a lot of stakeholders in hospital systems that are very interested in what we're doing," he said.

"It goes from physician contracting to compliance to procurement folks to, you know, all sorts of other positions. So you tell them about their risk, and there's no consulting that we do. We give them the outputs depending on what they put in," he explained.

"And we give them an idea of how to make sense of it all, after they get that output. They will hopefully start to collect data differently from providers and staff. That's part of what we can help them do. And we can help them manage those relationships differently," he added. "We look at what rules they are putting in place based on the data to reduce their risk and talk about new training components. A lot of providers have relationships with pharma and device companies and others. And many of these organizations would rather have it be out in the open and be able to show 'here's why this is beneficial to patients.'"

Changing tack slightly, Narva said: "Here's something interesting. Health systems in general spend between 10% and 20% of their total budgets on suppliers that have material relationships with staff. So, if you have a health system that's spending \$10 billion a year, they're going to be spending at least a billion dollars a year on suppliers that are actively trying to influence their staff, whether that's a good thing or not."

Businesses are paying attention

Narva said organizations that never previously thought about conflicts of interest are starting to pay attention, especially insurance companies – Medicare and Medicaid especially. Why? Because it's the appearance of one that we often discover rather than a true conflict, he said.

"Have you ever met an insurance company that wouldn't use the appearance of something untoward to push back on a reimbursement or

payment? No, that's risk and that gets factored into how much your policy costs you – it's how much the insurance company pays out.

"Think about Medicare advantage. They respect the number of dollars per patient, and if they see that there's \$4 per patient being spent that is potentially being influenced by a physician financial relationship, you think they're not going to push that button?" he asked.

"Now I am not going to sit here and tell you that conflicts of interest mean there's a definitive path where that conflict of interest will lead to a higher insurance premium. My role is merely to look at the data, see that a provider has a financial relationship and some behavior changed. That's all I can see and must manage. Then the organization has to analyze it. I'm not making the call," he reiterated.

This clarity in terms of not crossing reporting lines was a key message. "We tell firms 'listen, we found 14 things that we think you should look at in your audit, or we think that you should look at these items on an ongoing basis or get a little bit more information about them.'"

And referring back to what he said earlier, he added that it can also lead to lost money – organizations buying things they should not have bought.

Recordkeeping

Narva stressed that he tells organizations they need to manage their relationships, which means having some kind of documentation explaining how all the relationships work.

"So, for example, some hospital systems will not allow providers to utilize medical devices where they own royalties. OK, fine. But put into some sort of record that you know about this risk, have identified it, and have a document that governs this relationship. It's a risk, but it's been mitigated. It helps the organization say it has vaccinated itself against this reputational and regulatory issue."

Narva emphasized that it should be remembered that something might not be a conflict of interest, even though it really looks like one, because it is in the best interest of the patient or it really is the best solution.

"Let's say that a drug company comes out with a new drug that is better than any existing drug. And let's say that they have five prominent doctors who know all about this, and they want those doctors to

tell the world about how great this drug is. And they pay those doctors a lot of money to go to conferences and talk about this stuff. They are telling people about a better way of doing things. And that could be a good thing," he pointed out.

"But where you have a drug company that has a drug that is no better than any of the alternatives and costs 20 times as much as the alternatives – and the result is that doctors go from prescribing a generic version to this very expensive non-generic version – that's an example where there is a potential legal issue. Now there's a medical necessity issue and the decision is potentially being driven by a financial relationship or a kickback," Narva said.

What this means in 2025

Asked about his predictions for this year and beyond, in terms of compliance departments staying focused on risk mitigation as they got used to it, or whether they would be willing to take more risk, Narva said it was unclear.

"From a compliance perspective, I think it's hard to tell what exactly is going to happen in this administration and because of this administration. I think when it comes to conflicts of interest, this administration is clear about where it stands on conflicts of interest. There's a mention of conflicts of interest and research right in the Make America Healthy Again policy paper they issued.

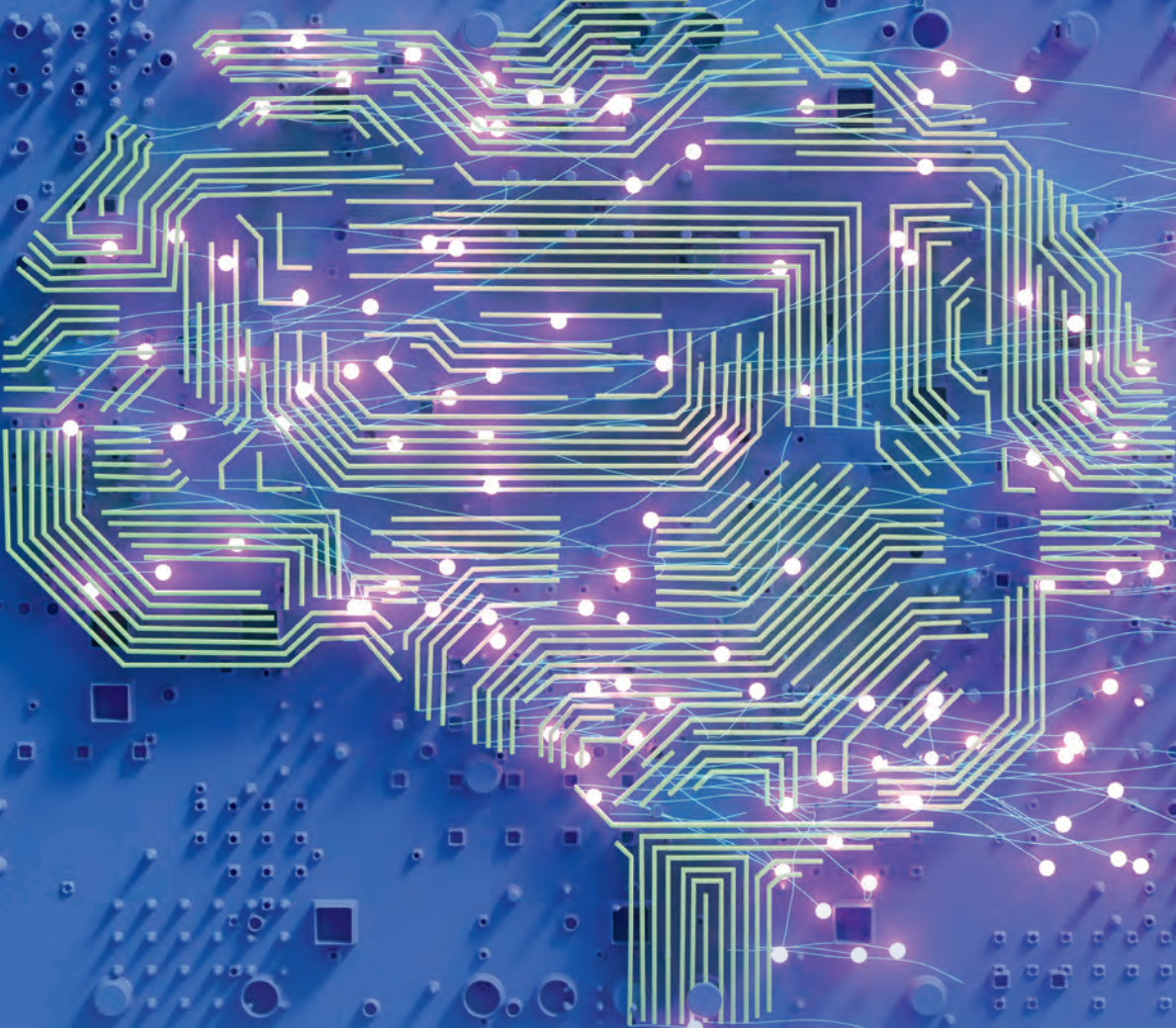
"And Marty Makary, who is going to run the FDA, is a guy who is very focused on waste and unnecessary prescription drugs. I think those things are aligned," Narva said.

"In terms of government spending, for every dollar that the government spends on healthcare enforcement, they make like three or four dollars back.

"Whether or not the Trump administration is pointing the light in the right direction is not really for me to say. But if they do something about the financial waste and streamlining costs, that is moving in the right direction in terms of healthcare outcomes."

Narva explained that what he called "the tail of wrongdoing" is long, and compliance officers know this. It would be unwise to take the foot off the pedal now in any risk area, he added.

"This administration will use what it has at its disposal to do what it wants to do. That's something people should think about carefully," he concluded. ●



The role of AI in driving healthcare compliance

The rapid development of artificial intelligence and its increased use in the life sciences sector are now major factors in the evolution of both industry compliance and government enforcement

SCOTT A MEMMOTT
& JONATHAN P YORK

The rapid development and growing accessibility of artificial intelligence (AI), and the expanding use of AI in the life sciences sector, are becoming increasingly important factors in the continuing evolution of pharmaceutical industry compliance, and government enforcement efforts.

But the use of AI comes with unanswered questions over its incorporation into both business operations and corporate compliance programs. If they haven't already, pharmaceutical manufacturers would be wise to begin tackling oversight of AI and consider the limited guidance on the use of AI in compliance programs from authorities such as the US Department of Justice (DOJ).

Given the continued claims from enforcement agencies such as the DOJ and the Department of Health and Human Services Office of Inspector General (HHS OIG) about investment of resources in their data-driven investigative techniques, pharmaceutical industry companies risk falling behind the government if they don't also take initial steps to improve the effectiveness of their compliance programs by including AI.

DOJ prosecutorial guidance

In September 2024, the DOJ Criminal Division issued an update to its Evaluation of Corporate Compliance Programs (ECCP) document, which is the Criminal Division's guidance for federal prosecutors as to the factors they should use to evaluate the effectiveness of corporate compliance programs. Although the ECCP is designed to inform the federal government's potential charging decisions related to and/or resolution of criminal cases, the questions the DOJ asks prosecutors to consider address underlying compliance principles from which corporations design, implement, and evaluate their compliance programs.

Guidance issued by enforcement agencies typically lags new technologies, but the DOJ appears to be trying to get out in front of – or at least keep pace with – the emergence of AI. The September 2024 update to the ECCP focuses extensively on new technologies in general and AI in particular, not only with respect to how AI is deployed in a company's business operations, but also how AI is incorporated into a company's compliance program to make the program more effective.

The ECCP defines AI broadly and states

that “no system should be considered too simple to qualify as a covered AI system due to lack of technical complexity,” including but not limited to machine learning and generative AI systems that operate with or without human oversight.

The use of AI in business operations

In determining whether a compliance program is appropriately designed to detect and prevent the type of misconduct most likely to occur at a particular company, the ECCP historically has directed prosecutors to consider traditional risk factors such as the industry sector in which the company operates, the regulatory landscape related to that industry sector, the competitiveness of the market, and a company's potential clients and business partners.

With the September 2024 update, however, the ECCP now instructs prosecutors to also consider AI, and other new and emerging technologies that a company and its employees use to conduct company business; whether the company has conducted a risk assessment with respect to the use of that technology; and whether the company has taken appropriate steps to mitigate any corresponding risk to ensure compliance with its own code of conduct and all applicable laws, specifically including any impact on the company's ability to comply with criminal laws.

When prosecutors assess whether a company has implemented adequate controls around the use of AI in business operations, the ECCP suggests that prosecutors ask, among other technology-related questions:

- ◆ whether the management of risks related to use of AI and other new technologies is integrated into broader enterprise risk management strategies;
- ◆ what the company's approach is to governance regarding the use of new technologies such as AI in its commercial business;
- ◆ whether controls exist to ensure that AI is used only for its intended purposes;
- ◆ how the company curbs potential negative or unintended consequences resulting from the use of AI;
- ◆ how the company trains its employees on the use of AI and other emerging technologies.

It's likely that few pharmaceutical industry compliance programs have attempted to identify whether and how AI is being used in a company's business operations, let alone to assess whether

it has answers to the questions posed by the ECCP. It would be prudent for pharmaceutical industry compliance professionals nevertheless to use the sections of the ECCP related to emerging technologies to guide compliance program development and operations.

The DOJ is not likely to look favorably on companies that have barreled ahead with the use of AI or other new technologies without considering compliance risks and implementing commensurate controls, particularly if the technology is the source of, contributes to, or facilitates fraud. And despite the framework established by the ECCP for evaluating corporate compliance programs, it remains to be seen how government enforcement and regulatory agencies actually will assess how a company manages risk related to ethical use of AI and other new technologies.

It will be necessary, therefore, for companies to be inventive in how they identify, assess, and mitigate such risks, at least in the short term.

The use of AI in compliance programs

Separately, the ECCP clearly communicates an expectation that compliance programs be designed and operated with AI in mind. The ECCP suggests that prosecutors assess whether a company is using new technologies such as AI in its compliance program, whether the compliance program is monitoring such technologies used by the business to evaluate whether they are functioning in a manner consistent with the company's code of conduct, and the speed with which the company can detect and correct decisions made by AI that are inconsistent with the company's values.

Again, it's likely that few pharmaceutical industry compliance programs have thought about these issues, let alone begun to incorporate AI into the operations of the compliance program itself.

The ECCP underscores that stakeholders in the pharmaceutical industry have an opportunity to assess, design, and improve their oversight of business use of AI and other technologies while recognizing the uncertainty and challenges such technologies present.

Effective monitoring and auditing is one of HHS OIG's seven elements of an effective compliance program. Companies in the pharmaceutical industry will need to address how oversight of AI technologies, something that HHS OIG has not specifically addressed to date »

with respect to compliance program guidance, fits into their broader auditing and monitoring functions. Stakeholders in the pharmaceutical industry have an opportunity to assess, design, and improve their oversight of business use of AI and other technologies while recognizing the uncertainty and challenges such technologies present.

Compliance programs will need to determine how AI technologies can best be used to enhance compliance auditing and monitoring, how the compliance program effectively governs and monitors its own use of AI, and what risks are presented by the double-layered approach of AI-assisted monitoring of AI-assisted business operations.

The ECCP also instructs prosecutors to assess how other traditional elements of an effective compliance program have been adapted to new and emerging technologies, such as updating policies and procedures to address risks associated with the use of new technologies; ensuring compliance personnel have appropriate experience and qualifications appropriate for AI and other new technologies; and whether a compliance program has appropriate funding, resources, and access, including whether compliance personnel have knowledge of and the means by which to access all relevant data sources in a timely manner.

Data-driven enforcement

Pharmaceutical manufacturers risk falling behind law enforcement and regulators if they delay investing in these compliance opportunities. The industry has for years heard representatives from DOJ and HHS OIG threaten increased scrutiny and analysis of the wealth of data available to the government, especially from government healthcare programs like Medicare and Medicaid, to identify potential fraud and abuse.

There are some indicators that this increased focus on data is being used to at least initiate enforcement actions under laws such as the False Claims Act (FCA). It's unclear whether this emphasis on "home-grown" FCA investigations based on data analytics will be a continued focus under the new US administration, but the tools and infrastructure will be available to and likely will continue to be used by the DOJ and HHS OIG.

The most recent FCA recovery statistics, however, show a continued rise in FCA



Recent actions involving COVID-19 programs offer an example of the government's use of AI and data to combat fraud

whistleblower complaints, which may similarly be fueled by private parties' use of AI tools such as large-language models to analyze large sets of publicly available data.

Data as a contributor to pandemic-related fraud

Although not directed at the pharmaceutical industry in particular, recent investigations and enforcement actions involving COVID-19 programs, such as the Paycheck Protection Program (PPP), provide examples of the government's use of data analytics to combat fraud.

The Pandemic Response Accountability Committee's (PRAC) Pandemic Analytics Center of Excellence (PACE), an analytics hub of data scientists and investigative analysts tasked to identify potential fraud in data associated with pandemic relief programs, drew praise and bi-partisan support from the Biden administration and members of Congress. PACE marshaled vast amounts of resources and data through 47 Memorandums of Understanding with corresponding Office of Inspectors General and law enforcement agencies to support over 700 pandemic-related investigations.

In 2024, the Biden administration and Congressional leaders expressed support for continuing and even expanding the PRAC and the next generation of PACE to apply to all federal spending, and although it's unclear at this point whether this effort will continue under the new US administration, it certainly is consistent with the administration's many public announcements about eradicating fraud, waste, and abuse in government programs.

It's unlikely that regulators and law enforcement are not going to continue using the advancements and vast

resources available to PACE, even as the country moves further away from the COVID-19 pandemic. Indeed, DOJ representatives have recently touted "aggressive" continuing enforcement efforts under the FCA.

Key takeaways

Stakeholders in the pharmaceutical industry must navigate the incorporation of AI and related technologies into their businesses, including as part of their compliance programs.

This may not be a simple endeavor, as the pharmaceutical industry will need to consider the regulatory implications of such technologies across regulated areas, and not just with respect to the ECCP. For instance, the industry will need to consider the FDA regulatory status and privacy implications of any integrated technologies.


Yet, without more definitive and formal direction to the industry from federal agencies, pharmaceutical companies should consider the questions presented in the ECCP for use by federal prosecutors and any other preliminary guidance pronouncements in carefully evaluating and developing internal controls governing the use of AI and other new technologies in their business operations. And in deploying AI to enhance the effectiveness of compliance program operations.

To do otherwise could have serious consequences. Because data sharing and analytics across government agencies appear to be permanent tools to be used by enforcement agencies such as the DOJ and HHS OIG, the pharmaceutical industry would be well advised to begin mitigating the risk by using similar AI and analytics-based strategies in their own compliance programs to identify similar indicators of fraud and to therefore preempt any potential investigations and/or enforcement actions. ●

Scott A Memmott is a partner at Morgan Lewis and represents life science and healthcare organizations in government and internal corporate investigations. Jonathan P York, also a partner at Morgan Lewis, represents US corporate clients, government and internal investigations and complex litigation.

The views expressed are those of the authors.

New leadership at US agencies (such as DOJ and HHS) mean vastly different priorities at them might currently apply that do not align directly with the ECCP when it was published.



Complete solution

End-to-end compliance
for total efficiency



25 years of innovation



Integrated solutions



Regulatory expertise



Single vendor efficiency



24/7 support



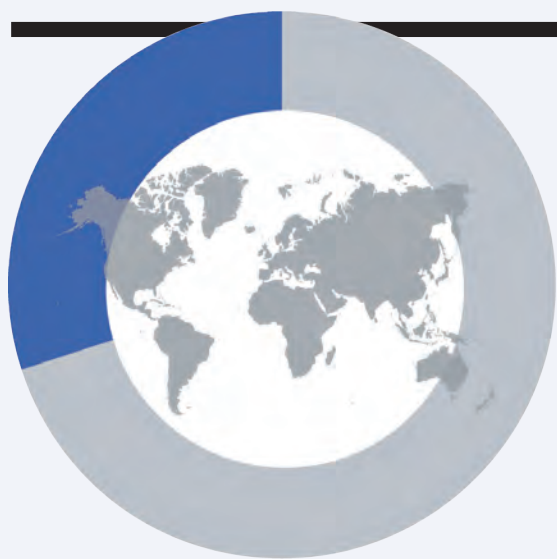
Unmatched security

Complete communications compliance



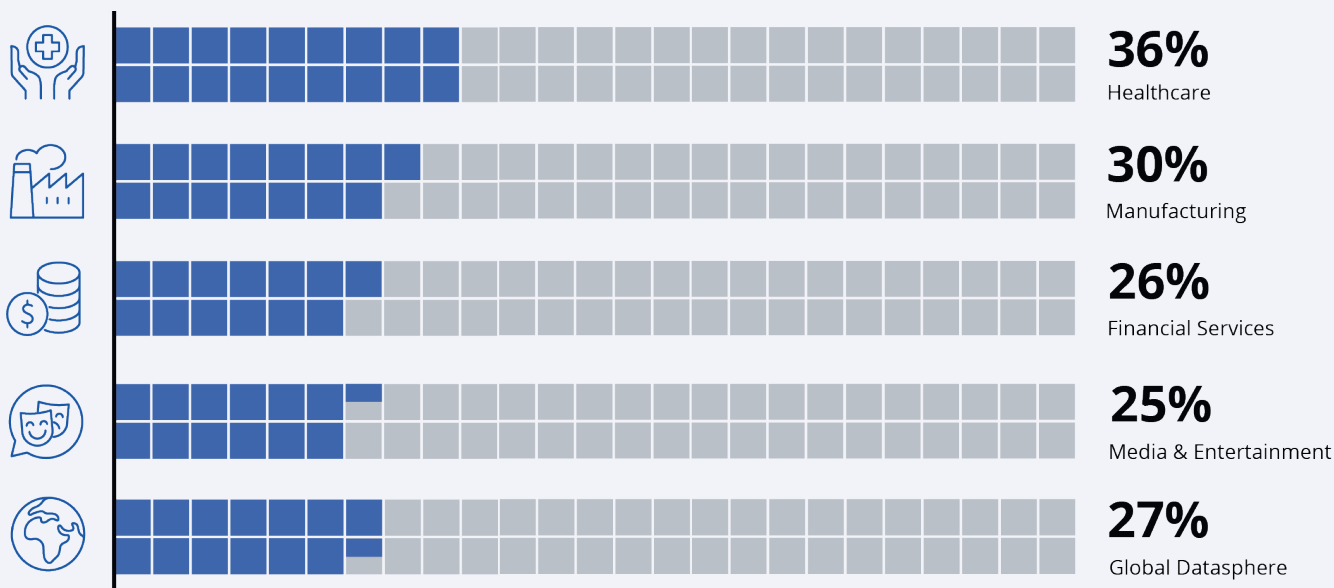
global**RELAY**

THE WEALTH OF DATA ABOUT HEALTH



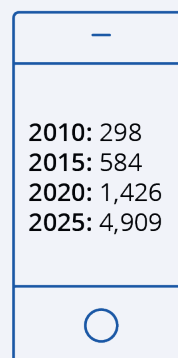
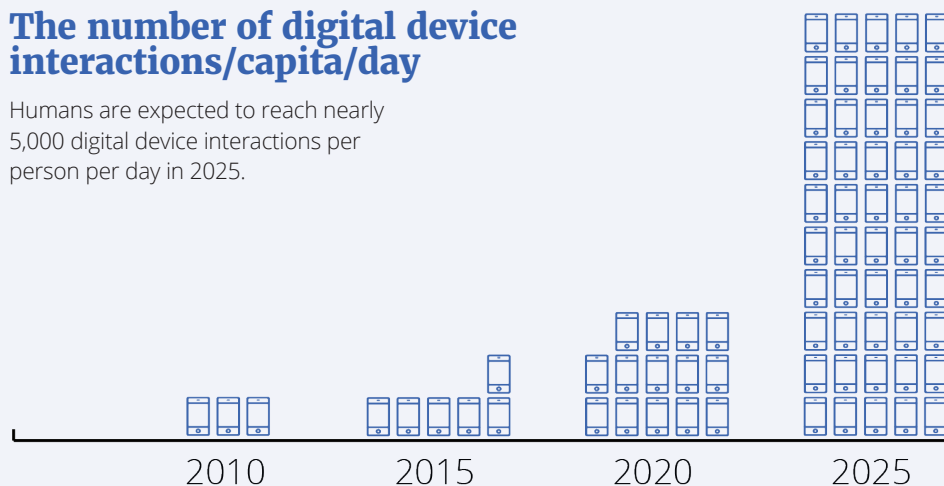
30%

Today, approximately 30% of the world's data volume is being generated by the healthcare industry. By 2025, the compound annual growth rate of data for healthcare will reach 36%.



The number of digital device interactions/capita/day

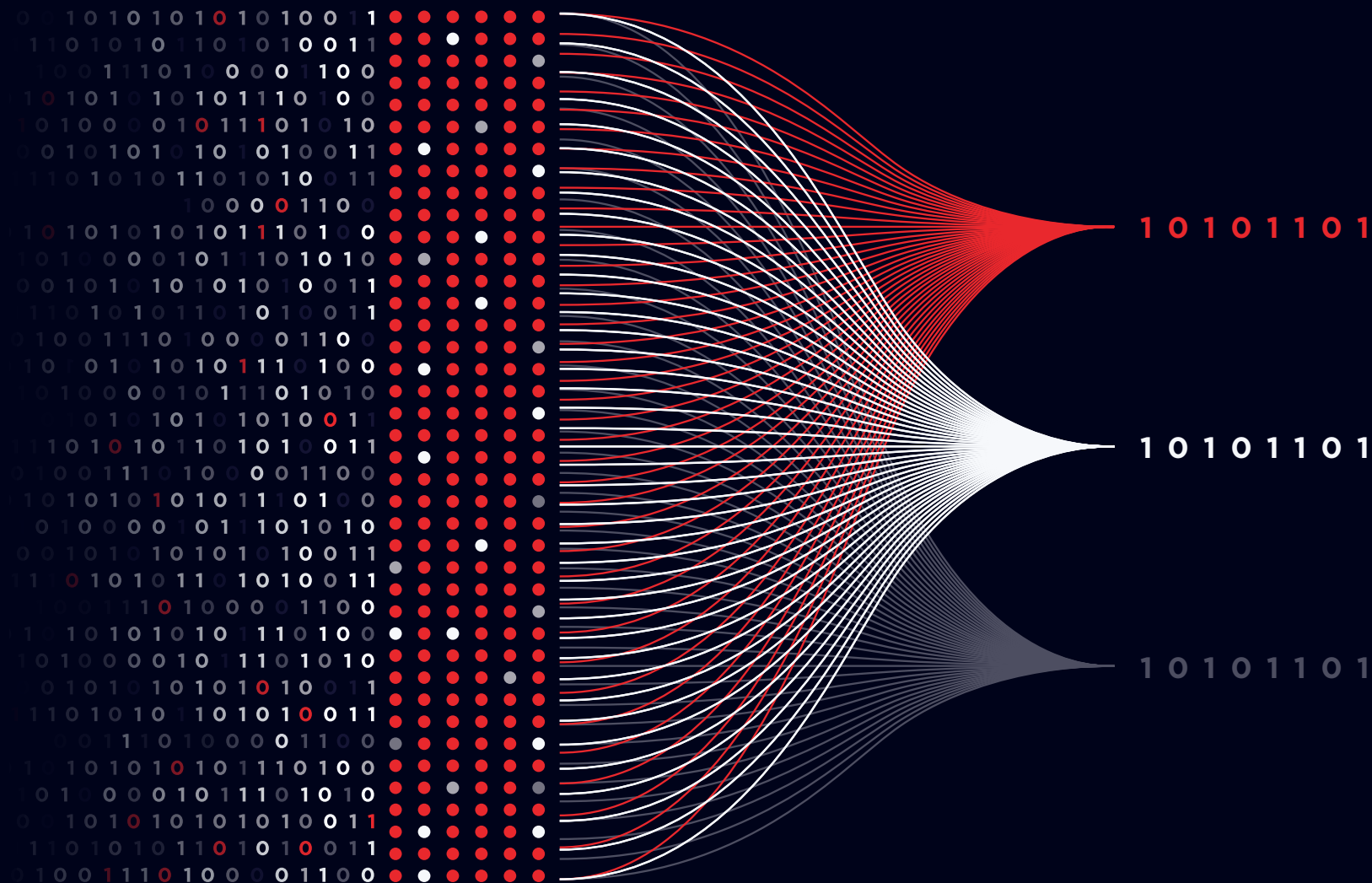
Humans are expected to reach nearly 5,000 digital device interactions per person per day in 2025.



Source: RBC Capital Markets

Every communication channel, captured & consolidated.

Global Relay Connectors streamline and archive your
communications data for complete, actionable compliance.



Capture everything.
Find anything.



Grip.

Get practical insights on the latest developments in compliance and technology

Visit GRIP, Global Relay's new digital information service with daily business content on key headlines and trends in the rapidly shifting compliance landscape.



For a limited time, we're offering a free trial of our new subscription content service. Check out GRIP today:
grip.globalrelay.com