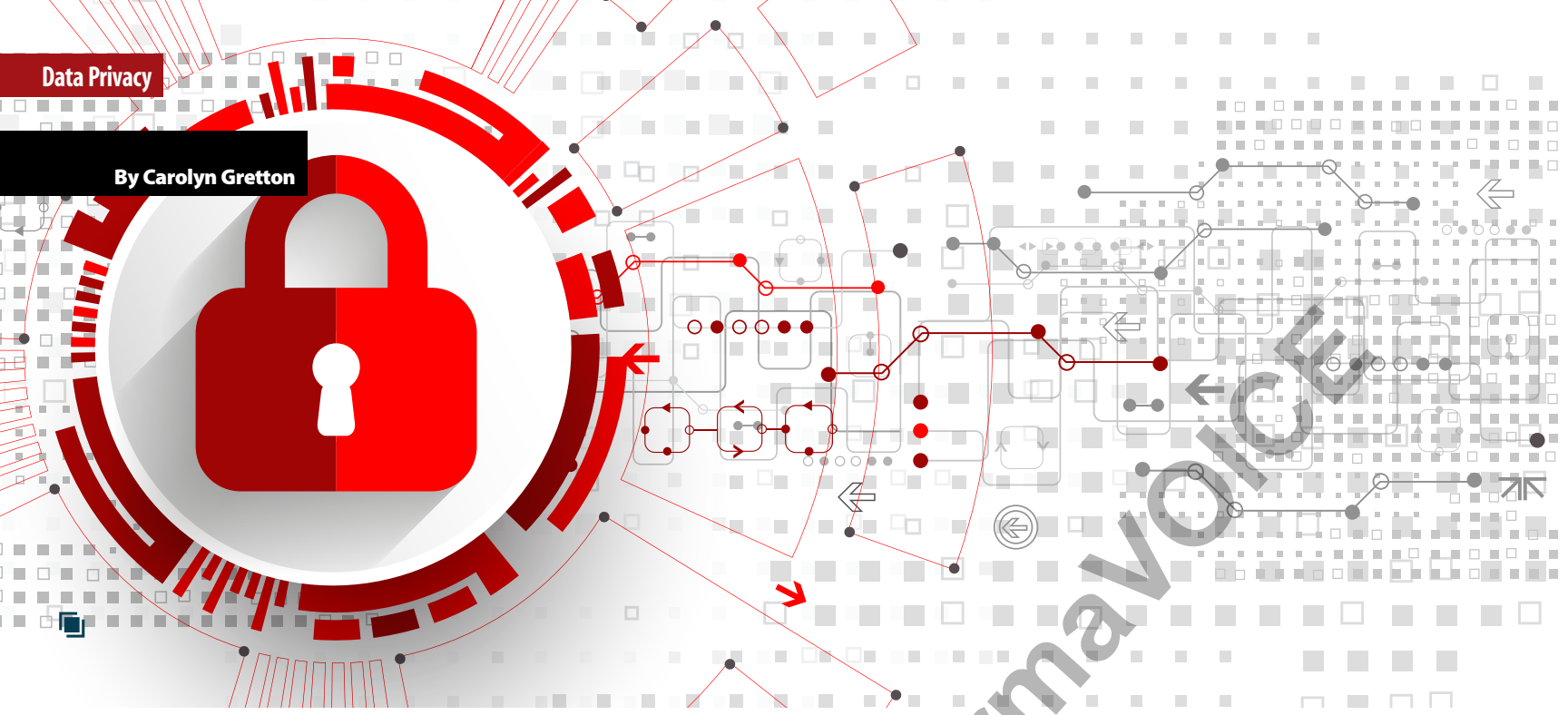
By Carolyn Gretton



Data Privacy: A Delicate Balance

The recent advent of new, portable digital health technologies and the increasing involvement of tech giants such as Google and Facebook in mining healthcare data have brought the issue of data privacy front and center. Constant interaction with digital devices that monitor, measure, and analyze various aspects of health and give third-party companies access to this information — as well as the changes in data collection and transmission forced by the COVID-19 pandemic — are transforming the entire concept of data privacy and raising questions as to how best to protect this data going forward.

Scott Taylor, chief privacy officer in Merck's Ethics & Compliance Office, agrees the data privacy field has been going through unprecedented changes. "Globalization, coupled with greater computing power, advanced analytics and algorithms, observational data, and more ubiquitous data sharing due to digital ecosystems, has not only strained traditional tenets of privacy laws and regulations, but has resulted in an overall erosion of trust among many data subjects," Mr. Taylor says.

"Although these trends are less common in our industry, the impacts spill over," he adds. "Data subjects can see the results of observational data, and the worries they have are leading legislators and regulators to react through more restrictive laws and regulations."

According to Mr. Taylor, one difficulty with today's privacy laws and regulations is that they were designed for a pre-digital environment, with tenets founded on notice and consent, as well as a focus on individual autonomy and empowering each person to control the collection and processing of their data. "Consent will always play an important role, but it is much less effective in the observational data collection and advanced analytics world we find ourselves in today," he says.

> NEW DIGITAL HEALTH TECHNOLOGIES AND INCREASED AWARENESS ABOUT PUBLIC HEALTH DUE TO THE COVID-19 PANDEMIC ARE PAVING THE WAY FOR A FUNDAMENTAL SHIFT IN HEALTHCARE DATA PRIVACY.

"From targeted digital recruiting to wearable biometric devices, the spectrum of technology-led solutions and vendors is vast," says Jen Davis, deputy general counsel and privacy officer at Science 37. "A single patient in a single study might have multiple digital touchpoints — each for a different purpose and each from a different platform — so there's an urgent need to ensure patient privacy throughout the drug development process."

Data Privacy and COVID-19

As is the case in most areas of healthcare and the life sciences, COVID-19 has left its mark on data privacy. Michelle Hoiseth, chief data officer at Parexel, notes that in its efforts to respond quickly to COVID-19, the global life-sciences industry has been required to push past its historical concerns and accept some risk to data privacy introduced by new technologies and the expanded sharing of healthcare data.

"People became very vocal about how they wanted healthcare data to be used," Ms. Hoiseth says. "The adoption of technologies such as privacy preserving proximity tracing apps, which would have previously been viewed with risky 'big brother' concerns, have been incredibly robust, which tells us that, for the right reason, people want us to find safe ways to use their data for the greater good."

"The pandemic has led to the generation of huge quantities of data for a brand-new disease in record time — be it through real-world data collection, clinical trials for therapeutics, or clinical trials for vaccines," says Anne Heatherington, Ph.D., senior VP and head of Data Sciences Institute (DSI) with research and development at Takeda Pharmaceuticals. "In my view, data privacy in these scenarios has neither been compromised nor advanced with this data generation."

Hayes Williams, Ph.D., head of data governance for Daiichi Sankyo, believes that COVID-19 accelerated trends that were already in progress in terms of increasing efforts to manage data remotely and securely.

"A good place to look at how this is taking shape is to examine how the phar-

Compliments of PharmaVOICE

(c) PharmaLinx LLC. Rights do not include promotional use.
For distribution or printing rights, contact mwalsh@pharmavoice.com

maceutical industry interacts with third-party organizations such as contract research organizations (CROs)," Dr. Williams says. "Before the pandemic, it was conceptually easier for the sponsoring pharma company to perform in-person check-in activities to ensure the CRO was adhering to privacy and other data requirements. But in-person check-ins are sometimes not possible or at least harder in these times, which forces companies to accelerate their remote monitoring and check-in capabilities. This includes a focus on ensuring that data follows privacy restrictions end-to-end even when it is not possible to see the process 'with your own eyes.'

Globalization, coupled with greater computing power, advanced analytics and algorithms, observational data, and more ubiquitous data sharing due to digital ecosystems, has not only strained traditional tenets of privacy laws and regulations, but has resulted in an overall erosion of trust among many data subjects.

SCOTT TAYLOR
Merck

"In the future, there will obviously need to be increased focus on technological tools and capabilities to help manage critical personal data in both the sponsor and CRO environment to ensure data privacy rules are managed remotely in both partner environments," he continues. "Data will need to be managed in a consistent and responsible way, including approaches that include data-masking and anonymization as minimum-use principles. Bottom line, if a company has a clear process and approach that is trusted to help confirm third-party adherence to data privacy and data management standards, the whole process will be more efficient, resulting in lower costs to both the company and CRO."

Ms. Davis says one positive byproduct of this devastating pandemic has been the increased willingness of biopharma companies, academic medical centers, CROs, and regulators to share internal data and resources to address urgent public health need.

"Although this need related to the COVID pandemic will subside eventually, we do expect to see continued growth in the number of assessments, standards, and policies to ensure robust data privacy protection while allowing for appropriate, population-based research to support other and future public health issues," she says.

"There have been some instances of relaxation of privacy protections in connection with COVID-19 data sharing where there are public health concerns, so long as the data sharing is reasonable for the circumstances," says Kim Gray, chief privacy officer at IQVIA. "This flexibility will be temporary, however.

"Balancing the need to support public health and also protect individual privacy has been challenging, with tremendous variances in attitudes and requirements by global data protection authorities and other regulators on how best to find equilibrium," Ms. Gray says. "This tension will not go away when COVID-19 is managed; lawmakers and regulators around the world will not reach consensus on the appropriate approach."

According to Ms. Davis, recent data protection legislation shows continued support of patients having more and easier control over their personal health information. "At the same time, the pandemic has helped to highlight the positives of sharing one's health information to benefit others," she says. "In addition, the pandemic has shown the clear benefit of participating in a clinical trial, not only for the individual participant, but for the broader community that benefits from the information learned from the study as well."

Keeping Employee Data Private

Alpesh Patel, chief technology officer at Orbita, notes a major element of the COVID-19 pandemic has involved the rapid transition in work settings from physical offices to remote, work-from-home environments. "The percentage of employees working from home has increased from 33% to 61% throughout the pandemic," Mr. Patel says. "This has required significant changes to accommodate the new normal and highlights the need for many organizations to reevaluate how their data is protected and close any existing security gaps.

"For example, telemedicine and virtual healthcare options have introduced new elements to consider around data privacy and security, such as enabling all available privacy and encryption modes for these virtual visits," he continues. "As some privacy and security regulations loosened to enable virtual care options, other regulations needed to rise to reduce these potential gaps in protection."

"In terms of routine clinical care, we did see shifts that required clarifications to data privacy around areas such as telehealth, safety of first responders, and walk-in clinics," Dr. Heatherington says. "The opportunity afforded to us with COVID-19 is around the rapid integration and understanding of the data, as well as the need to evaluate appropriate data sharing mechanisms across the ecosystem, particularly by more novel means."

The adoption of technologies such as privacy preserving proximity tracing apps, which would have previously been viewed with risky 'big brother' concerns, have been incredibly robust, which tells us that, for the right reason, people want us to find safe ways to use their data for the greater good.

MICHELLE HOISETH
Parexel

Mr. Patel says the heightened attention around security in telehealth and in remote work environments will extend beyond the pandemic. "While certain objectives may change, increased innovation and digital expansions will augment the need for existing security solutions," he says. "Throughout the COVID-19 pandemic, the concept of contact tracing has sparked conversations around data security and privacy and sheds light on the need for improved methods of health-related information-sharing and tighter security."

At Merck, Mr. Taylor says the scope and scale of the pandemic required all nonessential workers to shift to remote working almost overnight, creating immediate issues for network access loads, cybersecurity, and privacy.

"With so many people working remotely, the need to monitor expanded and had to be deployed in different ways," he says. "The technical issues can and have been solved, but ensuring we protect our environment and data to new vectors while respecting the privacy of our workforce and visitors has taken some focused work and partnerships internally. We have developed comprehensive privacy guidance related to impacts from the pandemic,

Compliments of PharmaVOICE

(c) PharmaLinx LLC. Rights do not include promotional use.
For distribution or printing rights, contact mwalsh@pharmavoice.com

Balancing the need to support public health and also protect individual privacy has been challenging, with tremendous variances in attitudes and requirements by global data protection authorities and other regulators on how best to find equilibrium. This tension will not go away when COVID-19 is managed; lawmakers and regulators around the world will not reach consensus on the appropriate approach.

KIM GRAY
IQVIA

ranging from health and wellness monitoring for employees, contractors, and visitors who need to be on site, to contact tracing and monitoring, to back-to-the-office protocols."

Ms. Gray says the balancing of public health and privacy during the pandemic has been highlighted most acutely in the employment context.

"Employers have needed to strike a balance between protecting the health and safety of their workforce while also protecting individual privacy," she says. "For example, when an employee tests positive for COVID-19, care must be taken to disinfect the area visited by the employee, which requires knowing where the employee passed through, and to protect co-workers who may have been exposed to the infected employee, which requires knowing the employee's contacts.

"At the same time, the employee's personal health information has always been considered private information, not to be shared with anyone except with the employee's permission," Ms. Gray adds. "Tensions between employment law and privacy law have required creative solutions."

"In privacy law, concepts have always existed to allow for a balancing of the fundamental right to privacy against other fundamental rights," Mr. Taylor says. He cites Recital 4 of the EU's General Data Protection Regulation (GDPR), which conveys that data protection is not an absolute right, but that any decisions in the use of data must serve the people.

"In the past, we have seen events like terrorism put these concepts to the test in the balancing of individual privacy rights against the rights to safety and security," he says. "The pandemic is having similar impacts, and governments are trying to appropriately balance the privacy rights of individuals against the fundamental rights to public health, safety and security, employment, and education. We have seen different approaches and inconsistencies by governments to date, but we believe this will get better with time and global cooperation."

"Employers now have an increased interest in their employees' health information to fulfill business needs like predicting resource challenges and maintaining business continuity, and to ensure a safe workplace environment," Ms. Gray says. "Yet an employer may need to treat its employees differently depending upon the employees' home country. Asking an employee if he or she is symptomatic or has tested positive for COVID-19 is forbidden in some countries. Taking an employee's temperature, even in a contactless manner, is prohibited in some countries and required in others. In all cases, employers will need to properly safeguard any employee information collected."

Mr. Taylor says in the short term, many of the data privacy challenges have been accommodated under broad requests by governments to comply with public health requirements. "But the pandemic will have long-term impacts, such as a shift to more remote working than we saw before the pandemic," he says. "Once the public health issues start to resolve, governments and companies will need to ensure their approach and methodologies strike the right balance between monitoring and privacy protections for individuals.

"Even once the disease is brought under control, its impact will likely transform how we live and work in the future, such as greater work from home accommodations; greater use of telemedicine, which has expanded significantly during the crisis; and public health measures on industries like travel," he continues.

A Need for A New HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in the 1990s, a time when most healthcare data was kept on paper. And while its privacy and security provisions were updated in the early 2000s to extend to electronic health records, it has not kept pace with the seismic changes that have occurred in the ubiquity and availability of healthcare data.

Mr. Taylor observes that all privacy and data protection laws, including HIPAA, will need to be modernized to accommodate the increasing availability and collection of data as the digital ecosystem continues to evolve. According to Mr. Taylor, the HIPAA Security Rules currently:

1) Establish national minimum standards for protecting personal health information (PHI) held in electronic form
2) Mandate technical and non-technical safeguards that must be in place to secure electronic PHI
3) Provide flexibility so that covered entities can implement varying policies and procedures based on the entity's particular size, structure, and risks while being technology-neutral

"While encryption of PHI data is the standard today for transmission security, encryption at rest of such data should also be considered for inclusion in HIPAA in light of both the increase in data breaches and to align with the supplemental measures to protect sensitive personal information as called for by the European Data Protection Board," Mr. Taylor says. "The limiting factor in any such change is the viability of homomorphic computing of encrypted data."

Mr. Patel notes the scope around why and how HIPAA is evolving is narrow at present. "To truly maximize and unlock the possibilities and opportunities around digital healthcare innovation, HIPAA-related regulations need to support a wider range of objectives," he says. "This involves strategic planning and alignment between covered entities, the government, and technology providers."

Ms. Gray says HIPAA was "designed to be flexible and agnostic" in terms of technology, so she doesn't believe changes to HIPAA related to digitization of healthcare data are the answer.

"The difficulty is that the scope of HIPAA doesn't capture much of the digitized consumer health data now readily available," she

Compliments of PharmaVOICE

(c) PharmaLinx LLC. Rights do not include promotional use.
For distribution or printing rights, contact mwalsh@pharmavoice.com

The pandemic has led to the generation of huge quantities of data for a brand-new disease in record time — be it through real-world data collection, clinical trials for therapeutics, or clinical trials for vaccines. In my view, data privacy in these scenarios has neither been compromised nor advanced with this data generation.

DR. ANNE HEATHERINGTON
Takeda Pharmaceuticals

says. "Expanding HIPAA's scope beyond data generated by plans, providers, and clearinghouses isn't really the answer either, given HIPAA's strong emphasis on the 'traditional' healthcare milieu. U.S. federal omnibus privacy legislation, harmonized with HIPAA, would allow for a more consistent approach to protecting healthcare information — and other kinds of personal information — regardless of the organization holding the information."

Dr. Williams says while new privacy laws should influence updates to HIPAA, he thinks the major additions to these laws will come from the explosion in new types of patient health data and the associated implications.

"New data types like various forms of genetic and related data -omics, such as genomic and proteomic data, are becoming more prevalent," he says. "Guidelines on how to manage this type of data need to be revised in a way that protects patients, and to an extent their families, especially since there could be potentially biasing information like 'tendencies towards' certain disease conditions. This type of information should be explicitly managed by that person.

"Wearable technology also provides another new data type that could have profound questions," Dr. Williams adds. "New smart watches are able to record blood oxygen levels. These data are then sent straight to a provider cloud and stored there. The licensing agreement signed by the user probably says this explicitly, but the terms in these agreements may not be easy to understand by the average user. Once the data from the wearable is on the platform of the company, they can potentially start looking for trends in the data."

For example, he says, decreasing trends in blood oxygen levels might be indicative of COVID-19 infection. To help with detection of this clear public health hazard, does the platform company have the right to look for changes in trends without your consent? Do they have the right to do it in aggregate or anonymized to spot trends in communities since they also have location data? When do I lose control and ownership of my data even if I agreed it should be stored separately? "These are key new data types that revised HIPAA legislation should address," Dr. Williams says.

Mr. Patel says temporary adjustments made to HIPAA amid the COVID-19 pandemic have highlighted key areas in need of reevaluation and update. "For example, the ability to seamlessly, yet safely, share patient information for treatment and care coordination is critical for continued digitization of healthcare data," he says. "Patients' ability to access their protected health information and the timeline of that process — typically 30 days — needs to be improved. Modifications within HIPAA will enable organizations and patients to reap the benefits of automation and continued innovation while safely sharing and storing data."

Dr. Heatherington says it is clear telehealth is here to stay even once the pandemic is over, so it is important to ensuring appropriate patient safeguards are in place — be it in routine clinical care or clinical trials.

"Under HIPAA, data may be de-identified in a myriad of ways, though not necessarily with the same rigor," she notes. "More robust/standardized de-identification standards should be in place for data collected during routine clinical care or for research purposes, which would allow for choice-based interoperability, such as the enhancement of clinical trial data with routinely collected real-world healthcare data from a participant's own device."

"The area of patient consent, including HIPAA but also beyond HIPAA, has to be re-evaluated to reflect the shared needs between healthcare and life science to use healthcare data to address a broader array of clinical research needs to provide more impactful care for patients," Ms. Hoiseth says. "There are still some fundamental legal issues such as who actually owns what data. There are also fundamental process requirements such as how to execute rights and requests to be forgotten. Putting the control of their healthcare data directly in the hands of patients holds real potential to advance these fundamental issues.

"Societally, we are all becoming more data literate simply through our daily lives," she adds. "We need to leverage that in our use of healthcare data."

Protecting Remote Data

The virtual aspect of clinical trials appears in two contexts today: remote monitoring of studies and remote/virtual study visits between a study subject and the study investigator/staff. Mr. Taylor notes that Merck has adopted the guidance issued in 2020 by the FDA and the European Medicines Agency (EMA) covering each of these issues.

"Monitoring of clinical studies is a legal obligation imposed on us as study sponsor to ensure the quality of the study site and its record keeping practices," he says. "No special consent of the patient is required, as monitoring has always been mentioned as a legal obligation within the informed consent and it does not directly affect the study subject — rather, only the sponsor's interaction with the investigator and site staff. The only new aspect under the current COVID-19 pandemic is that the monitoring occurs remotely/virtually."

Mr. Taylor says FDA and EMA guidance requires several considerations when conducting remote monitoring. "First, we must take a risk-based approach to the most urgent and important sites/protocols to be monitored," he says. "Second, the means by which the remote monitoring takes place must be secure from an IT and privacy perspective. Third, we must document the decision-making process to reflect the first two points mentioned."

Since visits impact the subject directly and as such are more intrusive, the FDA and EMA require clear notice of the remote/virtual visits be included in the informed consent and also require express consent be given by the patient. "Moreover, the technological standards employed by the investigator and site must meet specific standards to ensure the confidentiality of the patient's health information, with prior approval of the exact technology used required by the relevant ethics review board," Mr. Taylor says. "If the site does not have an approved system for the visits, the company has offered use of its approved systems to facilitate the approval of the study protocol and the enrollment of the first patient."

(c) PharmaLinx LLC. Rights do not include promotional use.
For distribution or printing rights, contact mwalsh@pharmavoice.com

Compliments of PharmaVOICE

"The benefits of virtual clinical trials include reduced costs, travel, and time requirements — but this also means that companies now require enhanced data protection," Mr. Patel says. "To support this, service providers must perform more risk assessments against processes that involve the tools and communication methods used to interact with patients.

"Based on risks identified in this context, controls should be implemented that focus on the patient's ease of use while maintaining a level of security that does not compromise the importance of data protection," he adds. "This is the ideal time for organizations to expand and explore commercially available solutions that offer reliable data protection in compliance with industry regulations."

"From an ethical standpoint, biopharma companies should continue to treat clinical trial participants' data as they do in any setting — with the highest degree of care," Ms. Davis says. "Respecting privacy will always be the right thing for biopharma companies to do, and although the methods or setting of a clinical trial may change some of its operational and technical aspects, it does not change the fundamental understanding that clinical trial data is highly sensitive and participants should have their privacy rights respected and protected."

"Smart, complete permissions management is the keystone to successfully enabling secondary use of healthcare data while managing privacy," Ms. Hoiseth says. "From this base, decisions are made on the use of technology, how datasets are prepared for use, where they are stored, and who performs the analysis. We need to take a holistic approach as opposed to reacting to individual technologies or data sources."

"In many respects, privacy protection in remote/virtual clinical trials is not very different from many of the current activities occurring in today's society," Dr. Williams says, adding a more remote approach is already being applied in work and finance activities.

"It is important to make sure the basics are intact, including secure systems, training for correct processes and procedures, and how to identify potential phishing and similar attacks," he says. "For the tools and technology specific to clinical trials, special attention needs to be paid to data integrity. For example, is the data recorded in a verifiable and time-stamped manner? Are changes or data movements tracked and relatable back to the source? Is there an inherent structure consistent from start to finish?"

Ms. Gray says in much the same way as they dealt with the need to support a remote workforce by considering security threats and maintaining the network, companies need to consider what the risks are for virtual trials and how to manage those risks. "A strong security posture and good cyber-hygiene form the basis for protecting privacy in a remote/virtual setting," she says.

A single patient in a single study might have multiple digital touchpoints — each for a different purpose and each from a different platform — so there's an urgent need to ensure patient privacy throughout the drug development process.

JEN DAVIS
Science 37

"Companies can also learn lessons from the traditional trial setting," Ms. Gray notes. "Privacy and data protection policies, procedures, and processes have long been in place at traditional sites; borrowing from these can be a starting point in creating a resilient data governance model for virtual trials."

Dr. Williams notes companies also need to ensure that any patient data is recorded in a way that minimizes risk. "This means to make sure to compartmentalize the data by taking patient information in one place and data in another and relating them only with an ID that does not carry any meaning and anonymize when possible — though this requires some thought depending on the data to be truly de-identified," he says.

"A major advantage of virtual data collection is that, in theory, there is a direct link between the patient and the clinical trial data repository," Dr. Heatherington says. "From a data integrity viewpoint, this is an excellent progression with many fewer opportunities for errors in data entry, for instance. From a privacy viewpoint, however, the direct link may be HIPAA-compliant, but depending on the method of de-identification applied and the underlying security of the data conduit, unintended data disclosures may occur."

Ms. Davis says at minimum, from a legal and compliance standpoint, biopharma companies and their associated vendors must always comply with applicable international, federal, and state privacy laws such as HIPAA and the GDPR. "Forward-looking organizations, however, should go far beyond these regulations and operationalize privacy principles such as Privacy by Default and Privacy by Design to ensure data privacy is protected throughout the life cycle of the participants' data," she says. "Companies should also assess their data inventory, systems security, and data breach plans regularly, and update as needed. At Science 37, we respect participants' fundamental right to privacy and are continually evaluating our technology and standardizing our procedures with protecting that right in mind."

"As organizations that are transacting around healthcare and clinical research data, we need more forward-looking data policies," Ms. Hoiseth says. "Today, the policies that we have around data privacy, data classification, security, and controls were all developed in response to a specific need, so they all got put into place in a silo to address a specific requirement and handling of data. We really need to step back and say, this is the data environment that we now operate in, so here are the requirements for us. What will I and what will I not do with data that is associated with PII — personally identifiable information? What will I and what will I not do when I link data to another dataset that could potentially reveal the identity of a patient? With that then, you can align everything else in your business."

Also, Dr. Williams says, companies should not forget about training the people handling the data. "Make sure adequate training and processes are built to drive consistency and adherence for those running the study, and make sure consent is clear and a lens towards privacy is built into the patient activities as well as making the patient informed within the scope of what is possible," he says.

The Future of Data Privacy

Given the increasing focus on data privacy, our experts foresee the next 12 months

Compliments of PharmaVOICE

(c) PharmaLinx LLC. Rights do not include promotional use.
For distribution or printing rights, contact mwalsh@pharmavoice.com

bringing new laws and regulations designed to protect patient privacy rights globally.

"While technically old news, the GDPR, HIPAA, and the California Consumer Privacy Act or CCPA have been the leading examples of a move in this direction," Dr. Williams says. "More recently, the Virginia Consumer Data Protection Act — VCDPA — has expanded their respective citizen's rights to control their personal information. Other countries such as Japan and Brazil have passed data privacy legislation as well."

"I believe the future will require laws to better address the nature of an Internet-enabled world," Mr. Taylor says. "And companies will need to continue to strengthen their privacy programs to address more than a liability-based approach — and embrace ethics and social responsibility as part of their decision-making in the collection and use of data. The healthcare industry is in a good position to assist public policymakers as they find ways to integrate new mechanisms and methodologies that will allow for the robust use of data but ensure responsibility and accountability in its use."

Ms. Davis says given the overall uptick in decentralized clinical trial (DCT) tools and methodologies, she expects to see an increased focus on navigating the nuances of various privacy regulations through an ongoing, multi-stakeholder collaborative effort to develop and operationalize new standards of privacy for clinical trial participants.

"As part of this focus, companies will continue adjusting to the Court of Justice of the European Union decision to invalidate the EU-US Privacy Shield [Schrems II]," she observes. "Companies that were not already using other approved mechanisms to transfer data from the EU to the United States will need to develop a privacy program that incorporates valid data transfer mechanisms."

Dr. Williams observes companies have already taken action to respond to privacy-related legislation by instituting a specific data privacy office or team to handle these matters. "Companies will need to create new or expand current cross-functional teams in order to continue expansion of processes, technology, and education so that there are many eyes throughout the organization to review and see data through a privacy lens," he says.

According to Dr. Williams, the data privacy group within a company will also need to work in conjunction with a comprehensive data governance program. "A corporate information security office should be involved in integrated privacy frameworks combined with consistent data governance frameworks," he says. "Solidifying the relationship and reach of this triumvirate needs to be the continued goal of all companies to respond to expansion in data privacy concerns in the coming year."

Ms. Gray predicts a greater focus on ensuring vendors and other third-party data processors have robust privacy and security practices and processes, driven primarily by two factors: the pandemic response of outsourcing more functions to be able to keep up with rapidly changing demands, often without thorough vetting of third-party data processors; and the Schrems II decision, which will require more rigorous due diligence related to data recipients, especially third parties.

"Schrems II also reinforces the recent trend towards data localization, with pressure being put on multinational companies to maintain servers in Europe and to avoid data transfers to countries not having attained adequacy determinations," she says.

"Further, with respect to adequacy determinations for cross-border data transfers, the United States will continue to propose federal omnibus privacy legislation that could improve the odds of gaining an adequacy determination and supplant the need for Privacy

Be thought-provoking.

Be here.

PharmaVOICE

THE FORUM FOR THE INDUSTRY EXECUTIVE

(c) PharmaLinx LLC. Rights do not include promotional use.

Shield II or other legalizing measures to allow free flow of data from Europe to the United States," Ms. Gray says. "Whether any of the proposed bills will be passed, however, will be dependent upon Congress' ability to work in a bipartisan manner."

Ms. Gray also believes there is likely to be increasing legislation being proposed by the states, especially if a federal privacy bill seems unlikely to pass. "States will continue to propose general purpose privacy laws as well as laws that are specific to particular types of data or particular situations," she says. "Whether these state laws will continue to grandfather exemptions for those companies covered by existing laws is uncertain."

"In the United States, we will continue to see the introduction of privacy legislation at the state level, and we expect to see companies working diligently to assess if and how such new legislation applies to them," Ms. Davis says. "Some state privacy laws allow for exemptions for data already regulated by the government — such as HIPAA and clinical research — but this isn't the case universally. And companies must carefully consider how each new law might apply to their business and to various elements of clinical trial conduct."

Mr. Taylor agrees that in the short term a patchwork of state laws and statutes will continue to emerge in the United States, highlighting the need for omnibus U.S. federal privacy legislation. "Globally, we will see countries aligning their national laws closer to the EU GDPR," he adds.

Ms. Hoiseth sees some opposing trends evolving. "In one direction, we will see in an increase in activity intended to better protect data privacy," she says. "In the U.S., we expect more states to follow California in creating their own legislation in this area. Outside of the U.S., we see trends toward creating limitations around where data can be analyzed, and increased requirements to access and process data. Privacy concerns about who has lawful access to our data and how they use it are amplifying across the world, as evidenced by recent issues associated with TikTok and the GAFA four.

"In the other direction, we see the interest and the means to promote the ethical and impactful use of private healthcare data," Ms. Hoiseth continues. "More sophisticated technologies to anonymize or pseudo-anonymize data — while still allowing for data to be interoperable — are gaining traction."

Regulation and legislation are also evolving to support advances in the way that we use patient data, Ms. Hoiseth says.

Throughout the COVID-19 pandemic, the concept of contact tracing has sparked conversations around data security and privacy and sheds light on the need for improved methods of health-related information-sharing and tighter security.

ALPESH PATEL
Orbita

"Regulatory bodies are focused on creating appropriate mechanisms and frameworks to support the secondary use of healthcare data," she adds. "We now see significant penalties defined for instances of 'data blocking' under the 21st Century Cures Act. The EMA's workshop on GDPR and secondary data use this past September really helped the industry explore the considerations. Taking a few steps back, we are seeing a maturation of our position on data privacy across the world from, 'We can't take the risk of using these types of data,' to 'How do we protect the rights and privacy of the individual, while facilitating the use of data for the greater good?'"

Mr. Patel notes the COVID-19 pandemic has accelerated the digitization of healthcare data and placed a spotlight on data privacy across industries. "With fewer data privacy regulations from the U.S. government, certifications such as ISO 27701 will become of high interest to the United States and other world markets," he says.

"In the next year, there will likely be heightened scrutiny of data privacy violations and events connected to trusted companies," he adds. "The rapid digital transformations of the past year have left some companies vulnerable to the possibility of breaches, requiring expanded security infrastructures to keep pace with innovation."

This may cause concern from subjects regarding how their data is being used, Mr. Patel says. "Consumer opinions about the security of their data will fuel the strengthening of some existing regulations and perhaps even the introduction of new standards," he says. "Even further, liabilities may shift between B2B vendors that hold private information regarding data subjects such as customers, employees, users, and members. Generally speaking, we will see reinvigorated attention to data privacy and security in the next year as digital options and innovations grow and expand."

Dr. Williams believes the industry may see an increased number of cases where fines are levied against companies not following enacted legislation. "Additionally, as more customers and patients make inquires to companies to learn more about how their information has been or will be used, and even request that their information be removed from future use, there is an increasing likelihood of complaints for improper uses of data or failure to respond in a timely manner," he cautions. "Companies may need to be ready to respond to these types of requirements."

Dr. Heatherington sees three trends on the horizon. "The first is the globalization of privacy protecting practices, or at least, our ability to better work within the differing global frameworks that exist to ensure appropriate safeguards are in place to protect patients and trial participants wherever they may be located in our global community," she says. "The second is a better understanding of the consent process around healthcare data and the sponsor's role in ensuring the appropriate use of those data. The third is understanding how we can better link research datasets, while protecting privacy appropriately. We have some excellent examples of this, such as from Sweden, where data from multiple sources can be linked via a unique patient identifier. But for other datasets, we are just beginning to understand how to do this appropriately, via tokenization, for instance."

Dr. Williams says it's also important to realize that focus on privacy is just good business.

"If it is clear that a company is actively managing patient or customer data, trust and goodwill follow," he says. "The tools and processes needed to manage data privacy also help the organization manage their data assets in a more consistent and transparent way, which actually tends to create more business value."

Compliments of PharmaVOICE

(c) PharmaLinx LLC. Rights do not include promotional use.
For distribution or printing rights, contact mwalsh@pharmavoice.com

momentum

INVITES YOU TO ATTEND OUR VIRTUAL EVENTS

NextGen Clinical Trial Innovation VIRTUAL SUMMIT

April 28-29, 2021 | Virtual Event

Re:Imagine Medical Device Marketing

April 28-29, 2021 | Virtual Event

2ND ANNUAL

Re:Imagine Pharma Marketing

May 18-20, 2021 | Virtual Event

2ND ANNUAL

Psychedelic Opportunity Virtual Summit

June 1-2, 2021 | Virtual Event

DECODING DIGITAL HEALTH FOR LIFE SCIENCES

June 15-16, 2021 | Virtual Event

momentum in partnership with PharmaVOICE

FEARLESS IN PHARMA

June 23-24, 2021 | Virtual Event

LIFE SCIENCES PUBLIC RELATIONS & COMMUNICATIONS SUMMIT

July 20-21, 2021 | Virtual Event

THOUGHT LEADER LIAISON ENGAGEMENT SUMMIT

July 28-29, 2021 | Virtual Event

REGISTER NOW

www.momentumevents.com

Compliments of PharmaVOICE

(c) PharmaLinx LLC. Rights do not include promotional use.
For distribution or printing rights, contact mwalsh@pharmavoice.com