Deloitte.

COVID-19 and Your Return to Work Strategy
Focus on data privacy implications

As society emerges from the COVID-19 pandemic, organizations will wrestle with complex questions around personal information (PI) and protected health information (PHI) collection, privacy, and transparency while finding a sustainable path to reduce virus resurgence, and reassure employees and consumers that measures are in place to suppress the risks associated with returning to normal operations.

Considerations

Potential new data processing use cases...

The nature of information sharing between governments, public health officials, technology providers, and customers/citizens has fundamentally changed:

- **Employers** may collect additional PHI from employees and consumers to adopt workplace safety
- **Hospitals** and other health providers may institute contact tracing (manual and/or automated) with smartphones and Bluetooth® to detect likely infected individuals
- **Airports and transportation hubs** implement health indicator screenings, such as temperature sensors, to curb travel of infected passengers
- **Government agencies** leverage proactive travel reporting and real-time geo-location monitoring to track disease spread and generate statistics
- **Businesses** implement ongoing online/virtual interaction between employees and consumers

...lead to heightened privacy challenges

- Creation of **large datasets of sensitive PHI** and the need for associated data protection, security, access, strong encryption, and other controls
- Increased **need for privacy and transparency** to employees and consumers about what new data is being collected, why, and how it's being used with regard to COVID-19
- **Robust training** for managers and on-the-ground personnel tasked with sensitive data collection
- **New, frequent data collection points** and **untested, rapidly implemented data lifecycle processes** that have not gone through appropriate security/privacy review
- **Clear data retention schedules** for new data collected
- **Explicit guidelines** for use and sharing of newly collected data (as with government authorities)
- Compliance with **global data collection** considerations, including disparate regulatory guidance

Resulting enterprise imperatives

Improved customer trust & relationships	• Gather and manage individual's consent; confirm data is leveraged in alignment with the consent collected • Overcommunicate new data collection practices and update privacy notices accordingly • Continue to offer individuals the right to access and erase personal information, as applicable • Corporate contact tracing applications to protect employees/limit exposure while reducing privacy impacts (opt-ins) • Utilize internal and public data lakes to address organizational challenges and drive valuable customer insights
Reputation for privacy leadership	• Own your privacy narrative– explain how you are protecting newly collected and existing PI • Be vigilant in monitoring third parties involved in the collection and/or processing of PI/PHI • Remain cognizant that the current environment may increase risk of wrongful treatment (e.g., discrimination / illegitimate uses of PHI) and take appropriate precautions
Resilient return to business operations	• Re-evaluate existing processes, incorporating additional privacy considerations, before resuming operations • Resume operations in a phased approach – start with higher-priority businesses or those with higher dependence for in-person interactions first • Address the need for ongoing capabilities to respond to potential recurrent outbreaks, including additional data collection and processing methods, even after COVID-19 subsides

⚙ Actions to consider:

▶ Respond – do today

- ✓ Determine what capabilities your organization will deploy to monitor health (e.g., temperature sensors)
- ✓ Explore existing contact tracing application programming interfaces (APIs)/services to understand feasibility of your organization's use
- ✓ Review Centers for Disease Control and Prevention (CDC) guidance on evaluation criteria[1] for digital contact tracing tools; adopt a tailored criteria for your organization
- ✓ Leverage existing privacy policies, processes, and infrastructure and take advantage of existing risk tolerance levels and associated controls
- ✓ Embed security and privacy-by-design protections into the new processes, practices, and systems that involves data processing
- ✓ Make privacy/security practices part of the marketing strategy for reopening

▶ Recover – do this month

- ✓ Review access management processes and bolster security controls (e.g., multi-factor authentication) to prevent inappropriate access
- ✓ Integrate new datasets into individual rights processes; reduce data, where possible, and implement end-to-end protections
- ✓ Consider integration with other enterprise data to increase enterprise responsiveness to potential future outbreaks
- ✓ Incorporate data flows/considerations into updated crisis response plans
- ✓ Keep a pulse on reinstated regulations that may have previously been relaxed
- ✓ Monitor customer engagement channels closely to identify risk early and protect brand
- ✓ Evaluate use of technologies to streamline processes and simplify data collection and related decision-making

▶ Thrive – do next month

- ✓ Communicate process changes to employees and customers for new steady-state operations
- ✓ Establish and monitor data retention and disposal parameters
- ✓ Work with technology providers to keep application security controls configured appropriately
- ✓ Don't become complacent on normal cyber hygiene – continue to perform ongoing penetration testing and vulnerability scanning to proactively mitigate threats
- ✓ Update data loss prevention (DLP) rules to accommodate additional/new datasets and assess opportunities to slow (or stop) data collection
- ✓ Re-evaluate data minimization and access control decisions to determine if updates are required for long-term process maintenance

[1]*CDC Preliminary Criteria for the Evaluation of Digital Contact Tracing Tools for COVID-19*

🎯 Key takeaways

The needs and sophistication of security and privacy programs will vary by organization and industry; however, organizations should recognize a phased reopening of the economy as an opportunity to not only get back to business, but to lay the foundation for a more resilient future.

① **Stay in lockstep with evolving regulatory guidance**

② **Reduce data footprints where possible**

③ **Take a phase-based approach to bring new processes online**

④ **Overcommunicate early and clearly on new data collection/use**

📞 Contact: Coronavirus Response | USCyberCoronavirusResponse@deloitte.com

Deborah Golden
Principal
Deloitte & Touche LLP
debgolden@ deloitte.com

Linda Walsh
Managing Director
Deloitte & Touche LLP
lwalsh@deloitte.com

Eric Bowlin
Partner
Deloitte & Touche LLP
ebowlin@Deloitte.com

Arun Perinkolam
Principal
Deloitte & Touche LLP
aperinkolam@deloitte.com

David Mapgaonkar
Principal
Deloitte & Touche LLP
dmapgaonkar@deloitte.com