Morgan Lewis

FAST BREAK: GLOBAL HEALTHCARE PRIVACY DURING COVID-19

Reece Hirsch, Dr. Axel Spies, Lauren Groebe, Jake Harper

July 22, 2020

Morgan Lewis

TODAY'S PRESENTERS

Reece Hirsch

Dr. Axel Spies

Lauren Groebe

Jake Harper

Global Healthcare Privacy During COVID-19

Topics to be discussed today include

OCR's exercise of enforcement discretion regarding HIPAA compliance

Privacy issues raised by COVID-19 testing in the workplace

Use of "everyday communication technologies" for telehealth

Differing privacy obligations of HIPAA covered entities and FTC regulated apps

Permitted disclosures by HIPAA business associates for public health purposes

COVID-19 Apps in the EU – Privacy Issues

HIPAA Privacy in the Time of COVID-19

While COVID-19 is a unique public health crisis, other emergency situations also test the limits of the HIPAA Privacy Rule.

HIPAA is not intended to be an obstacle to a healthcare organization's essential treatment, emergency response, and public health functions.

HHS Office for Civil Rights (OCR) has issued several bulletins, announcements and guidance documents.
https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html

OCR's Notification of Enforcement Discretion for Telehealth

March 17, 2020

Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency

OCR announces, effective immediately, that it will exercise its enforcement discretion and waive potential HIPAA violations against healthcare providers that serve patients through "**everyday communications technologies**" during the COVID-19 nationwide public health emergency.

https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

OCR's Notification of Enforcement Discretion for Telehealth (cont.)

- Applies to widely available communication apps like Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype
  - When used in good faith
  - For any telehealth treatment or diagnostic purpose
  - Regardless of whether the treatment service is directly related to COVID-19
  - Does not apply to "public-facing communication apps" such as Facebook Live, Twitch, and TikTok
- Providers encouraged to notify patients that these apps potentially introduce privacy risks
- Providers should enable all available encryption and privacy modes when using apps

California Executive Order on Telehealth

- On April 3, California Governor Gavin Newsom waived penalties under several CA privacy statutes, regulations and local ordinances for
  - Healthcare providers' unauthorized access or disclosure of patient information
  - Related to the "good faith" provision of telehealth services
- Telehealth services is broadly defined
- Scope of order is also broad, extending to
  - Government penalties
  - Damages awards, including in private class action lawsuits
  - Penalties for failure to timely notify individuals or government authorities of data security breaches

Business Associates and Public Health Disclosures

April 2, 2020

OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency

OCR states, effective immediately, that it will exercise its enforcement discretion and will not impose penalties for violations of certain provisions of the HIPAA Privacy Rule against healthcare providers or their BAs for the good faith uses and disclosures of PHI by BAs for public health and health oversight activities during the COVID-19 public health emergency.

https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-hipaa.pdf

Business Associates and Public Health Disclosures (cont.)

- April 2, 2020: *Enforcement Discretion for Business Associates, Continued*
  - Applies even if the BAA doesn't provide for this use/disclosure, and only if:
    - 1. The BA makes good faith uses and disclosures of PHI for public health and health oversight activities; and
    - 2. The BA informs the CE within 10 calendar days after the use or disclosure occurs (or commences, with respect to uses/disclosures that will repeat over time)
  - Examples include uses/disclosures for or to:
    - The CDC, or similar state public health authority, for the purpose of preventing or controlling the spread of COVID-19; or
    - CMS, or similar state health oversight agency, for purpose of overseeing and providing assistance for the healthcare system as it relates to the COVID-19 response

Business Associates and Contact Tracing

- An activity tracker app offered by a health plan to its members may collect geolocation data that is useful in COVID-19 contact tracing
  - Can this business associate share geolocation data with a state public health authority?
  - Yes, because the disclosure would be permitted for the health plan under HIPAA
- The app developer must notify the health plan within 10 days
  - The developer works with many covered entities so notification could be challenging
  - OCR is flexible regarding form of notification, can be an email
  - But BA needs to maintain documentation of the notice

OCR's Notification of Enforcement Discretion for Testing Sites

April 9, 2020

Enforcement Discretion Regarding COVID-19 Community-Based Testing Sites (CBTS) During the COVID-19 Nationwide Public Health Emergency

OCR states, effective immediately, that it will exercise its enforcement discretion and will not impose penalties for violations of certain provisions of the HIPAA Rules against healthcare providers or their BAs in connection with the good faith participation in the operation of a COVID-19 Community-Based Testing Site (CBTS) during the COVID-19 public health emergency.

https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-community-based-testing-sites.pdf

OCR's Notification of Enforcement Discretion for Testing Sites (cont.)

- April 9, 2020: *Enforcement Discretion for CBTS, Continued*
  - Applies to CEs, including some large pharmacy chains, and their BAs participating in the operation of COVID-19 specimen collection and testing sites
    - CBTS include mobile, drive-through, or walk-up sites that only provide COVID-19 specimen collection or testing services to the public
  - CBTS to implement reasonable safeguards to protect the privacy and security of individuals' PHI when performing COVID-19 specimen collection and testing
    - Minimum necessary
    - Set up canopies or barriers to provide privacy during collection of samples
    - Control foot and car traffic at point of service to create distance and minimize the ability of persons seeing or hearing screening interactions (6 feet)
    - Create a "buffer zone" to prevent members of the public or media from observing or filing, and post sign prohibiting filming
    - Provide Notice of Privacy Practices

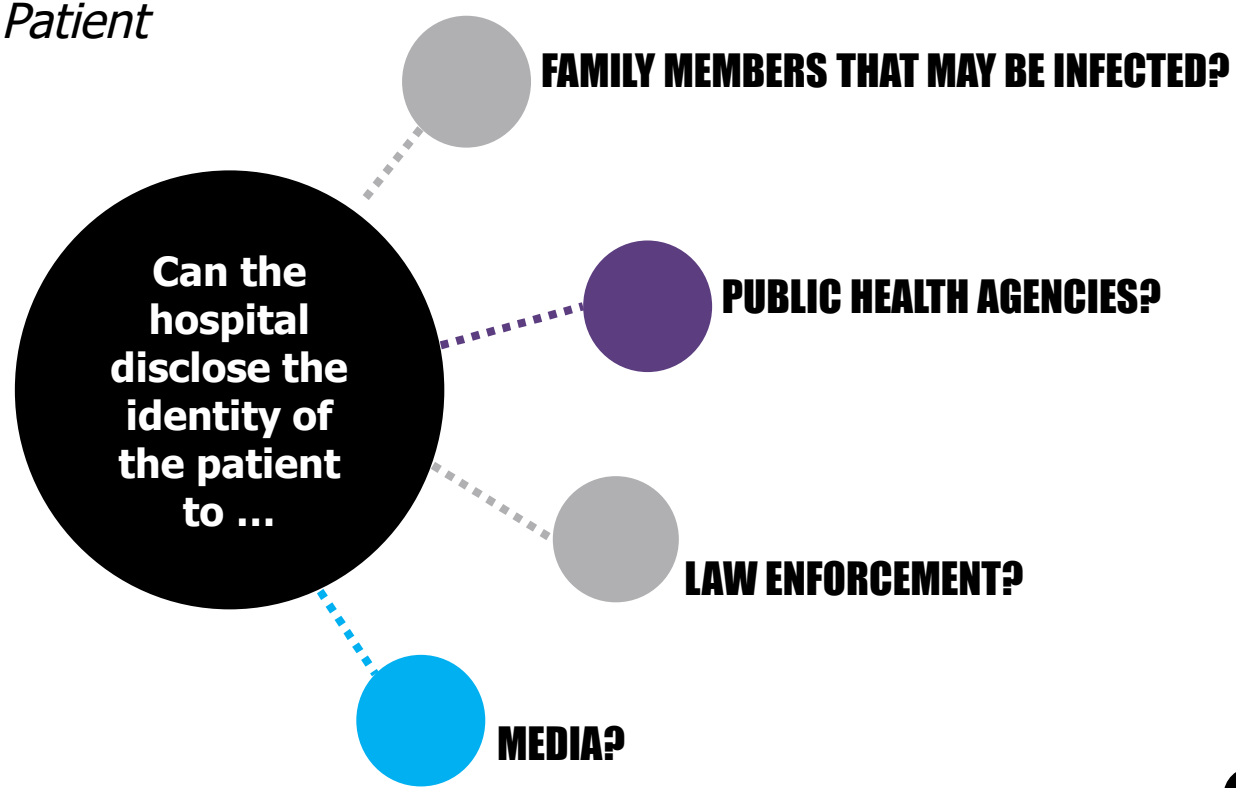
OCR's Notification of Enforcement Discretion for First Responders

- On March 24, OCR clarified that a covered entity may disclose PHI of an individual who has been infected with or exposed to COVID-19, without obtaining the individual's authorization, to first responders (law enforcement, paramedics, other first responder and public health authorities)
  - As necessary to provide treatment (such as disclosure to emergency medical transport personnel)
  - For public health purposes to public health authorities (such as CDC and state health agencies)
  - As required by law (such as state laws requiring reporting of positive COVID-19 tests)
  - To prevent or lessen a serious and imminent threat to health or safety (such as disclosures to child welfare workers and mental health crisis services personnel)

Privacy Issues raised by COVID-19 Testing in the Workplace

- *Hypothetical: Infected Patient*

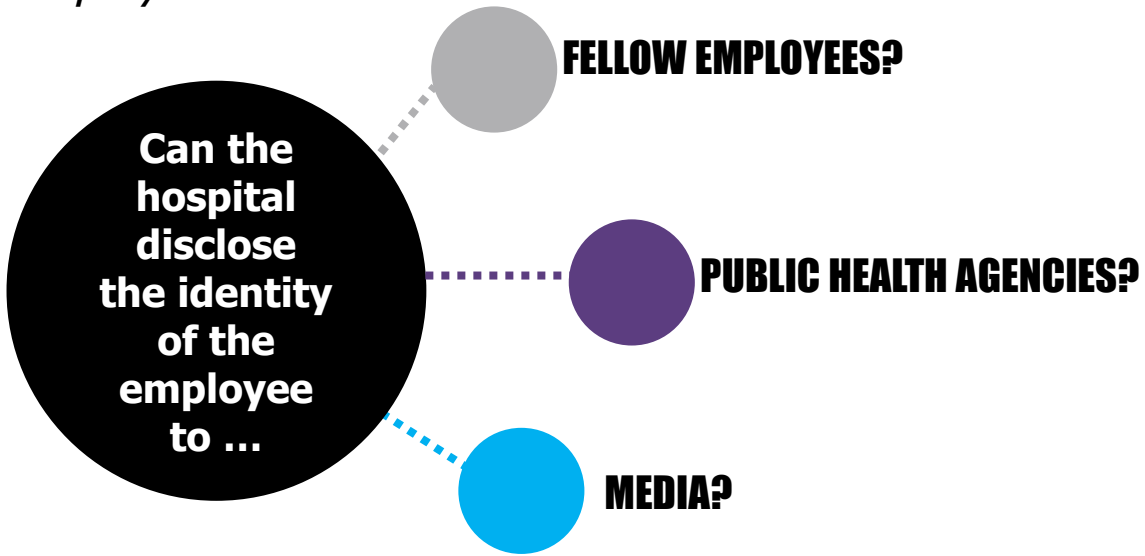
A hospital patient has tested positive for COVID-19



Privacy Issues raised by COVID-19 Testing in the Workplace (cont.)

- *Hypothetical: Infected Employee*

A member of the hospital's workforce has tested positive for COVID-19



*Remember that medical information received by the hospital in its capacity as an employer (rather than as a healthcare provider) is not PHI and is not governed by the HIPAA privacy rules.

Employee Privacy Concerns

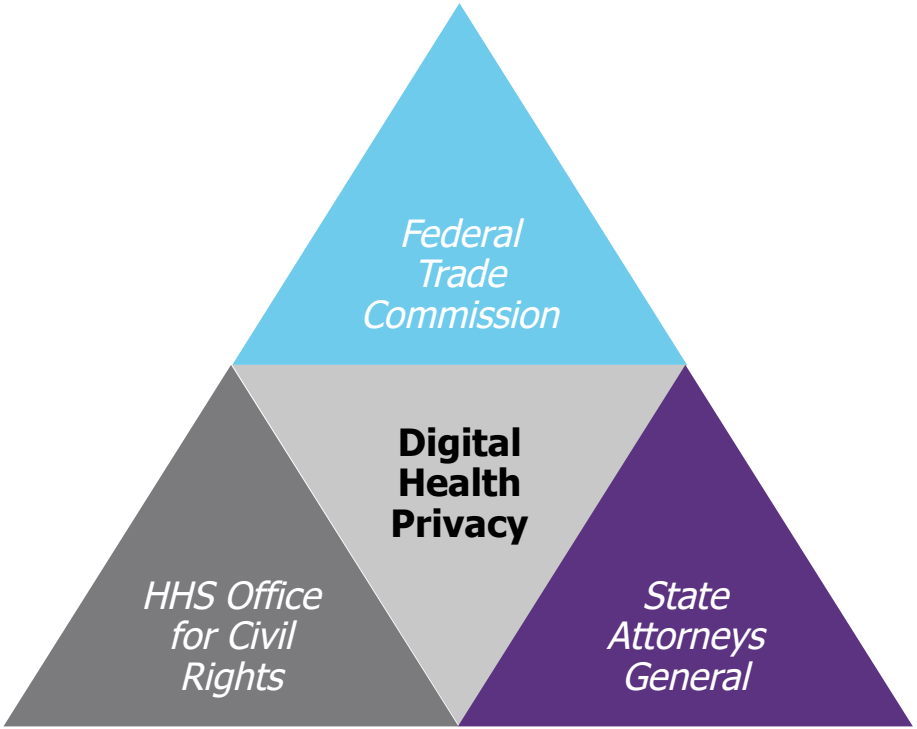
- As a general rule, an employer should NOT disclose the identity of an employee diagnosed with (or suspected of having) COVID-19
  - Under the Americans with Disabilities Act (ADA) employee medical information must be kept confidential and only shared in very limited circumstances
  - An inaccurate or false disclosure of someone's COVID-19 status could potentially subject an employer to common law defamation or invasion of privacy claims
- An employer should make every effort to protect the medical confidentiality of the employee while still providing sufficient information for other members of the workforce to take appropriate steps

Employee Privacy Concerns (cont.)

- If there's a subgroup of employees at higher risk of close contact with the affected person, HR should contact them separately to notify them of the risk
  - Affected employees will likely ask for the name of the infected individual
  - Unless the infected employee provides consent, the identity should not be disclosed, either directly or indirectly
- In an Interim Guidance for Businesses and Employers, the CDC states:
  - "If an employee is confirmed to have COVID-19, employers should inform fellow employees of their possible exposure to COVID-19 in the workplace but maintain confidentiality as required by" the ADA

The FTC and OCR

One overarching theme in (digital) health privacy is the overlapping jurisdiction of



The FTC and OCR

- FTC's authority to regulate privacy and security is under Section 5 of the FTC Act: "unfair or deceptive acts and practices"
  - An inaccurate or misleading statement or omission in a privacy policy, user interface or in other consumer-facing material can constitute a deceptive practice
  - Failure to have reasonable data-security practices, even in the absence of a deceptive statement
- OCR – regulates HIPAA covered entities
  - Healthcare providers that engage in standard electronic transactions; Health plans; Healthcare clearinghouses
- OCR also regulates business associates

OCR or FTC Regulation? Follow the Money

- Based upon a series of OCR guidance documents, it seems that one test for determining whether an app developer or other digital health company is acting on behalf of the consumer or the covered entity is:
  - Who's paying for the service?
  - If the consumer is your customer, you will probably be subject to FTC regulation, but not HIPAA
  - If the provider is your customer, you will probably be a HIPAA business associate
- Other resources:
  - FTC, OCR, and FDA developed a "Mobile Health Apps Interactive Tool"
  - OCR released "Health App Use Scenarios & HIPAA" (February 2016)

Contract Tracing and US Apps

A mobile health app that collects geolocation data may be useful in COVID-19 contact tracing programs

If the app is offered direct to consumers, FTC privacy principles apply

- App privacy policy should address the uses or disclosures of personal information for contact tracing or could be a deceptive practice in violation of Section 5 of FTC Act
- Three bills introduced in Senate would create greater protections for health data not regulated under HIPAA

If the same app is purchased by a hospital for its patients, then HIPAA privacy rules apply

- App provider may be a business associate and may rely on new discretion regarding BA disclosures to public health authorities

Privacy Issues raised by COVID-19

EU REGULATORS ADDRESS COVID-19 TRACKING AND TRACING APPS

EXAMPLES OF APPS: GERMANY AND FRANCE

EU Regulators Have Given Privacy Guidance

EUROPEAN DATA PROTECTION BOARD:

- Representatives of the national data protection agencies in the EU
- **Guidelines 04/2020** on the use of location data and contact tracing tools in the context of the COVID-19 outbreak
- Adopted: 21 April 2020 (relatively early)
- Legally not binding on the EU Member States
- Legal basis under the GDPR:
  - If the contact tracing application is processing sensitive data (**special categories of data**), like health data that identifies individuals:
    - Art. 9 para. 2 lit. i) GDPR for *reasons of public interest in the area of public health* or
    - Art. 9 para. 2 lit. h) GDPR for *health care purposes*.
    - Otherwise, processing may also be based on *explicit consent* pursuant to Art. 9 para. 2 lit. a) GDPR.

EU Regulators: Privacy Guidance (cont.)

EUROPEAN DATA PROTECTION BOARD:

- **Lawfulness, fairness and transparency,** Art. 5 para. 1 lit. a) GDPR → application's algorithms must be auditable + should be regularly reviewed by independent experts + source code should be made publicly available
- **Purpose limitation**, Art. 5 para. 1 lit. b) GDPR → exclude further processing for purposes unrelated to the management of the COVID-19 health crisis
- **Data minimization and Data Protection by Design and by Default**, Art. 5 para. 1 lit. c) and Art. 25 GDPR
  - The application should not collect unrelated or unnecessary information
  - Contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used
  - The collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.

EU Regulators: Privacy Guidance (cont.)

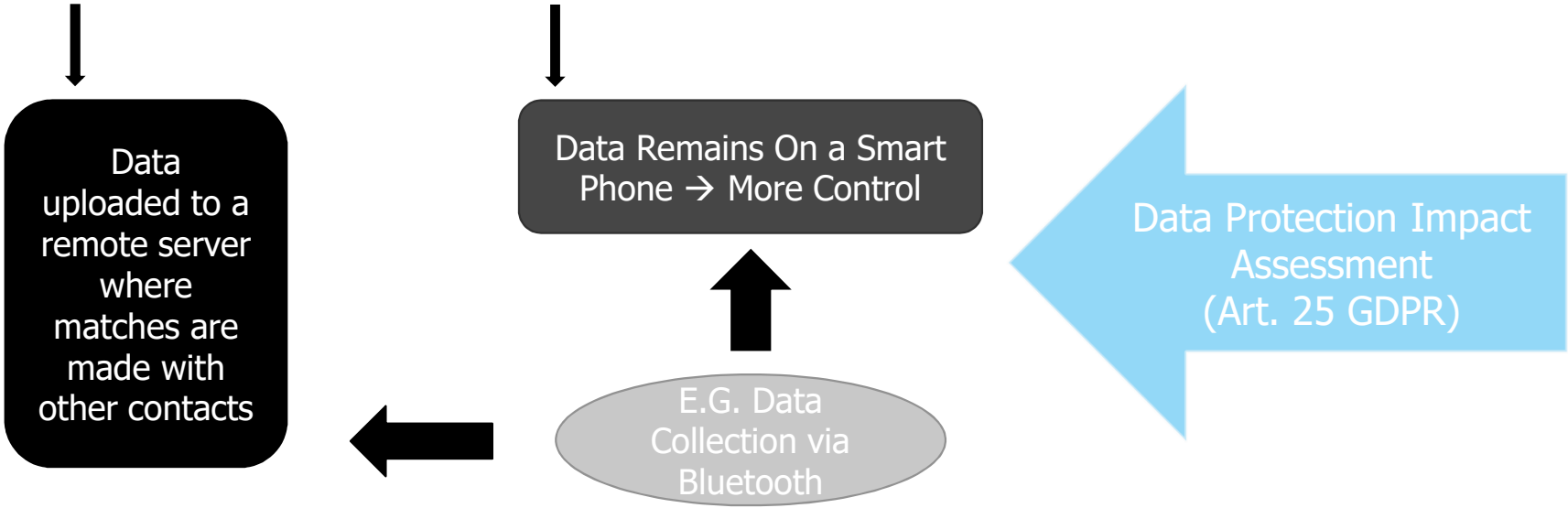
EUROPEAN DATA PROTECTION BOARD:

- **Storage limitation**, Art. 5 para. 1 lit. e) GDPR: With regards to data retention mandates, personal data should be kept only for the duration of the COVID-19 crisis.
- **Integrity and confidentiality**, Art. 5 para. 1 lit. f) GDPR:
  - Contact tracing apps should incorporate appropriate technical and organizational measures to ensure the security of processing.
  - Special emphasis on state-of-the-art cryptographic techniques which should be implemented to secure the data
- **Accountability**, Art. 5 para. 2 GDPR:
  - To ensure accountability, the data controller must be clear.
  - The EDPB suggests that national health authorities should be the controllers.

EU Regulators: Privacy Guidance (cont.)

EUROPEAN DATA PROTECTION BOARD: Functional Requirements

Centralized or a **decentralized approach -** both are possible under the GDPR



Processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution)

EU Regulators: Privacy Guidance (cont.)

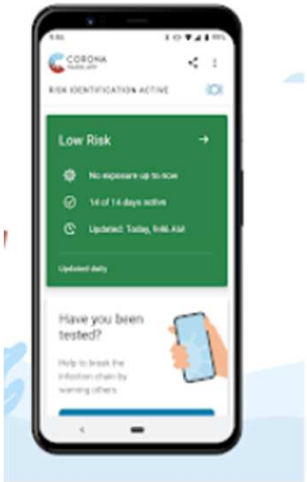
EUROPEAN DATA PROTECTION BOARD:

- Use of contact tracing applications should be **voluntary** and
- App should not rely on tracing individual movements but rather on **proximity information** regarding users.
- Authorities should not have to choose between an efficient response to the current pandemic and the protection of fundamental rights.

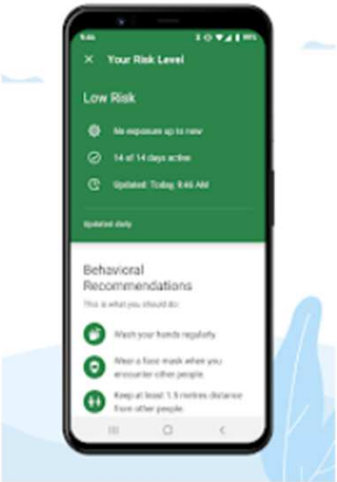
"Data Protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby to guarantee the effectiveness of the App."

German COVID-19 Warn App – Steps

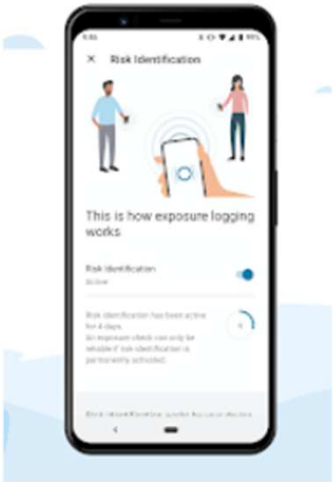
Check whether you had encounters with infected persons



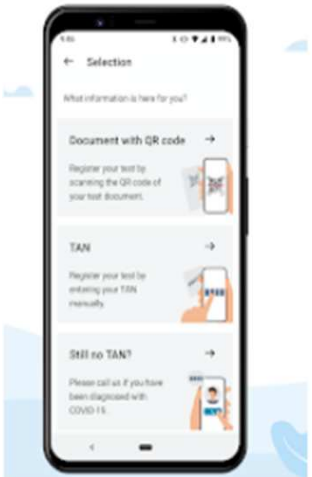
Learn how to act correctly in every situation



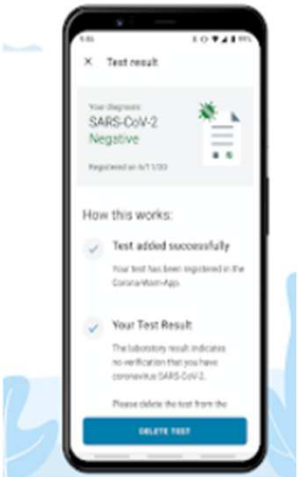
The app records your encounters – but no personal data



Users register their COVID-19 tests anonymously and warn others



Easily request your test result via the app



COVID-19 App in Germany

- So far the **most successful app** in the EU; free for users
- **Decentralized,** works via Bluetooth (issues)
- German government says the app cost €20 million ($22.7 million) to develop, and that it will need about €3 million per month to operate
- Downloaded since June 16: 14 million times in the first few days, now total of 16+ million, mainly thanks to German Government backing
- **Chancellor Merkel**: All Germany residents should take advantage of a COVID-19 app designed to "recognize and break up infection chains."

COVID-19 App in Germany – Issues

- Many people download it, but do not have Bluetooth switched on
- Multiple downloads counted as one?
- Bluetooth technology has limits (e.g. does not recognize screens)
- Employment law issues (private v. company devices)
- Some issues with "false positives" – City of Düsseldorf as an example.
- The digital connection between the app and the health authorities and laboratories via QR code does not work - at least not in Berlin.
- Apple version iOS 13.5 iPhone 6s released in 2015/ Android 6 Marshmallow and upwards supported – Some error messages

COVID-19 App in France – Issues

- "StopCovid", no tracking but tracing of contacts via Bluetooth as in Germany
- Doesn't run as background application
- Currently not compatible with the German App
- Different: Centralized data collection in France on a pseudonymized basis – CNIL Approval of 5/20/20 Délibération N° 2020-056 → No lists of infected persons may be downloaded
- French Bar Associations (*Barreau de Paris and Conseil National des Barreaux – CNB*) warn against using the App due to data protection concerns (Voluntary consent? Full anonymization of the data? Attorney-client privilege violated?)

Join us next month!

Please join us for next month's webinar:

***Fast Break:* What's Next: Managing COVID-19 Fraud Enforcement**

Featuring

Jake Harper, Tinos Diamantatos, Katie McDermott,
and Jonelle Saunders

- Tuesday, August 25, 2020 3:00 PM (EST)

Thanks and Be Well!

Reece Hirsch
Partner
San Francisco
+1.415.442.1422
reece.hirsch@morganlewis.com
Click Here for full bio

Reece Hirsch co-heads the firm's privacy and cybersecurity practice and counsels clients on a wide range of US privacy issues, specializing in healthcare privacy and digital health. Reece counsels clients on development of privacy policies, procedures and compliance programs, security incident planning and response, and online, mobile app, and Internet of Things privacy. In a Chambers USA ranking, Reece was recognized by his peers as "a consummate expert in privacy matters."

Thanks and Be Well!

RA Dr. Axel Spies
Special Legal Consultant
Washington, DC
+1.202.739.6145
axel.spies@morganlewis.com
Click Here for full bio

Dr. Axel Spies, based in Washington DC, has advised clients for many years on various international issues, including licensing, competition, corporate issues, and new technologies such as cloud computing. He counsels on international data protection (EU General Data Protection Regulation), international data transfers (Privacy Shield), healthcare, technology licensing, e-discovery, and equity purchases. Dr. Spies is co-publisher of the "German Journal of Data Protection" (ZD) and of "Multimedia Recht" (MMD). He is frequently quoted in the media for his telecommunications and privacy knowledge.

Thanks and Be Well!

Lauren Groebe
Associate
Chicago
+1.312.324.1478
lauren.groebe@morganlewis.com
Click Here for full bio

Lauren Groebe focuses her practice on regulatory and transactional matters affecting clients in the healthcare sector. She counsels hospitals, health systems, hospices, pharmacies, and private equity clients, among others, across a range of regulatory issues, including matters related to compliance with HIPAA, the 340B Program, the Sunshine Act, fraud and abuse laws, Medicare and Medicaid enrollment, and licensure requirements. Lauren also advises clients on the corporate and healthcare regulatory aspects of merger and acquisition transactions.

Thanks and Be Well!

Jake Harper
Associate
Washington, DC
+1.202.739.5260
jacob.harper@morganlewis.com
Click Here for full bio

Jake Harper advises stakeholders across the healthcare industry, including hospitals, health systems, large physician group practices, practice management companies, hospices, chain pharmacies, manufacturers, and private equity clients, on an array of healthcare regulatory, transactional, and litigation matters. His practice focuses on compliance, fraud and abuse, and reimbursement matters, self-disclosures to and negotiations with OIG and CMS, internal investigations, provider mergers and acquisitions, and appeals before the PRRB, OMHA, and the Medicare Appeals Council.