

NetDiligence®

**COVID-19:  
Global Privacy Concerns  
and Legal Ramifications**





# COVID-19: Global Privacy Concerns and Legal Ramifications

In the midst of the COVID-19 pandemic, the need for protected health information (PHI) to prevent disease spread is critical. Yet organizations must weigh this need against legal and regulatory requirements protecting individual privacy, said Shannon Yavorsky, partner at Orrick, Herrington and Sutcliffe and a leading authority on U.S. and European data privacy and security issues.

During the webinar “COVID-19 Emerging Issues: Managing Cyber Risks of a Remote Workforce and Global Privacy Concerns,” presented by NetDiligence and Arete Incident Response on March 24th, Yavorsky

explored the current legal and regulatory outlook in the United States and Europe vis-à-vis the coronavirus.

“Personal data is a valuable tool that can help inform decisions and policies and help reach specific and targeted conclusions,” Yavorsky said. “Yet it also presents substantial risk, to the individuals to which that data pertains, and to the organizations using it who are now operating under ever-increasing regulation.”

It is crucial now for companies to understand what medical information can be collected and shared, and what laws govern such use—

from giving notice and obtaining consent to data retention. Both the United States and the European Union have updated their regulatory requirements and standards to reflect the emergent health crisis. This paper covers the key recent developments and what organizations should do to stay compliant.

## U.S. Legal and Regulatory Overview

Within the United States, the main regulation touching health data is HIPAA, but there is no federal data protection law in the United States, making it what Yavorsky called a “patchwork” legal framework, with a mix of FTC and state laws.

“PHI is considered more sensitive data and presents relevant risks to data breach liability exposures with respect to class action lawsuits,” she said. Organizations need to be mindful of this.”

The Centers for Disease Control and Prevention and the U.S. Equal Employment Opportunity Commission have advised employers to keep certain personal health data confidential and most organizations have committed to keep employee, customer and user personal health data confidential as well.

California has led states on these issues, with two major pieces of legislation. The Confidentiality of Medical Information Act

(CMIA) defines medical information as “any individually identifiable information, in electronic or physical form, *in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor* regarding a patient’s medical history, mental or physical condition, or treatment.” “Individually identifiable” means that the medical information includes or contains any element of personal identifying information to allow identification of the individual, such as the patient’s:

- name
- address
- email address
- telephone number
- Social Security Number
- other information that, alone or with other publicly available information, reveals the patient’s identity

Generally, the California Consumer Privacy Act (CCPA) does not prohibit businesses from collecting personal information. Medical information subject to the CMIA is excluded from CCPA. However, Yavorsky noted that [businesses subject to the CCPA](#) that directly collect medical data from California employees without the involvement of healthcare professionals may not be able to rely on this exception.

“In that case, the business’ [notice at collection](#) should cover this information and describe the purpose for which that information will be use,” she said. “The same

may be true for California businesses that, for example, are directing security personnel to collect temperatures from non-employee visitors to their facilities.”

Given the developments of COVID-19, the U.S. Department of Health and Human Services’ Office for Civil Rights in Action has issued a [bulletin](#) on how HIPAA comes into play with the virus. Covered Entities can now share PHI without patient authorization or consent to the following:

- parties involved in treating the patient
- public health authorities
- foreign government authorities at the direction of public health authorities)
- at-risk individuals
- parties involved in patient care
- parties whose knowledge of PHI would lessen or prevent threats to public health and safety of others

Nevertheless, identifiable PHI is not permitted to be disclosed to media or the public and such PHI can’t be freely disclosed for other purposes. The rule of thumb is the “minimum necessary” standard: Covered Entities should make a reasonable effort to only disclose the minimum necessary amount of information needed, including in infectious disease reporting.

## Data Collection

Yavorksy noted some key risk mitigation tactics for companies collecting additional personal information during the COVID-19 outbreak:

- Give notice of data collection and use practices.
  - ! Be cautious about language used—for example, don’t state that data will be processed if it’s used for real time monitoring.
- Implement reasonable security protocols and data minimization efforts appropriate to the sensitivity of the data for its collection and storage, such as:
  - Encryption
  - Data separation
  - Data access controls
- Minimize data to be collected and shared.
- Anonymize data where possible
- Retain data for only as long as it needs to be retained.
- Revisit employee handbooks and privacy policies to ensure current practices are consistent with stated terms of use and revise them if necessary.

# Employers and Data

Organizations can minimize risk around PHI and data security by taking the following measures:

## 1. Assess communications.

- Educate the organization about security plans, policies and procedures.
- Create proper communication channels and information flow.
- Determine what health data can be shared with employees and the public.
  - Don't reveal identities of individuals who are under investigation for exposure to COVID-19.
- Continue due diligence around the collection, use and storage of employee health information.
- Update employees on latest COVID-19 news and prevention efforts from CDC.

## 2. Align information security policy.

- Revisit current policies for remote work, including access to company systems. If there are no policies in place, establish basic guidelines for remote access and the use of personal devices for company business.
- Assure employees their data will continue to be protected and secured.
- Review and remind the organization's privacy policy.



- Reevaluate data breach and incident response plans to ensure that they reflect current data breach and cybersecurity concerns.

### 3. Develop secure remote working arrangements.

- Train employees about remote work policies and provide guidance where needed.
- Monitor networks and access for anomalies

### 4. Evaluate third-party relationships.

- Examine security policies of vendors and business and strategic partners that involve the transfer, sharing or release of employee or customer data.
- Ensure third parties have authentication and access controls in place for sensitive data.

presents added risks such as race/ethnicity, political affiliations, and sexual orientations and health data. The EDPB and many European data protection supervisory authorities have released guidance on processing personal data in connection with COVID-19.

The new EDPB COVID-19 Guidance reaffirms the legal grounds for enabling health data processing without consent. At the same time, data controllers must still comply with the law when processing data. Additional rules as per the ePrivacy Directive now apply. The use of location data requires consent, or it must be anonymized. Emergency legislation can be introduced if it constitutes a "necessary, appropriate and proportionate measure" for public security.

The EDPB's COVID-19 Guidance remains focused on the principles of proportionality and the minimization for employee data. However it's important to note that while these laws are generally harmonized across the European Union, member states can derogate from the law in circumstances of "public interest," such as a global pandemic, making it critical for organizations to stay abreast of member state authority guidance as it's released in a rapidly changing regulatory landscape. To date, the member states that have released guidance include:

- |           |              |
|-----------|--------------|
| • Denmark | • France     |
| • Germany | • Ireland    |
| • Italy   | • Luxembourg |
| • Norway  | • Poland     |
| • Spain   | • UK         |

## European Union Legal and Regulatory Overview

The European Data Protection Board (EDPB) released updated guidance on data processing with respect to COVID-19. The European Union is suspending the General Data Protection Regulation (GDPR) and loosening restrictions on the processing of "special categories" of personal information, limiting data that

# EU Member State Employer Data Guidance for COVID-19

Specific regulatory authorities have detailed how employers can interact with data as related to the virus.

- The Danish Supervisory Authority urges employers to limit the collection and disclosure of data while allowing employers to collect data on:
  - Employee visits to high-risk areas
  - Employees maintaining quarantine
  - Employee illnesses
- The French Supervisory Authority urges employers to collect data that is only necessary to assess an individual's exposure to COVID-19 while allowing employers to:
  - Implement measures to prevent contamination and train employees
  - Raise employee awareness and invite them to provide health data
  - Facilitate communication channels and remote working
  - Document potential contamination
- The German Supervisory Authority only allows the disclosure of personal data of suspected or infected persons only if exceptionally necessary to prevent spread. It encourages the focus of data collection with the principles of proportionality and lawfulness but allows the access of health data to:
  - Prevent or contain virus spread among employees
  - Identify visitors who may be infected
  - Be retained if it aligns with purpose of containing spread of COVID-19
- The Irish Data Protection Commissioner underlines core GDPR principles in data processing such as:
  - Lawfulness, transparency, data minimization and accountability
  - Emergency data processing allowed to protect "vital interests" of an individual
- The Italian Data Protection Authority initially advised that that data processors refrain from processing health data concerning symptoms of COVID-19. It later changed the position and:
  - Allows the processing of health data when necessary to prevent spread
  - Offered a protocol that allows employers to collect and process health data with some conditions:

- Employee and visitor temperatures can be monitored in an anonymous manner.
- Employee and visitors can be asked about their movements in the past 14 days before allowing them to access the workplace.
- Data subjects must be notified before data is processed.
- Health data should not be disclosed to third parties other than the Public Authority.
- The Luxembourg Supervisory Authority published guidance stipulating that employers:
  - Should not require daily employee temperature checks or questionnaires
  - Should not require visitors to sign statements certifying their health conditions or travel to high-risk zones
  - Should ask employees about possible exposure
  - Should create channels for transmission of information
  - Should promote remote working arrangements and the use of occupational medicine
- The Norwegian Supervisory Authority defined "health data" relative to the virus—health data can include infection status but not travel to risk areas and quarantine status. It also specifies that employee infection or quarantine status should not be disclosed to outside parties.
- The Polish Data Protection Authority issued a statement clarifying data protection provisions:
  - Cannot be an obstacle for fighting COVID-19
  - Should follow recommendations and instructions of the Chief Sanitary Inspector and Prime Minister
  - Can impose specific preventative and control obligations on organizations
  - Data processing is lawful under GDPR as it is necessary for protecting vital interests
- The Spanish Supervisory Authority's statement and report stipulates that:
  - Preventative measures must comply with GDPR Spanish Data Protection Law and Spanish sectoral health laws
  - Companies must demonstrate a legal basis for processing health data and must minimize data processed as per the standards set by GDPR

- The U.K. Information Commissioner's Office issued a statement and FAQs for organizations:
  - The government, NHS and health professionals are not prohibited from sending public health messages by phone, text or email as such messages are not considered direct marketing.
  - Data protection should not stop organizations from sharing information quickly, but data processing should be proportionate in connection to COVID-19.
  - FAQs reassure organizations that regulatory action should not be a concern during the health crisis.
  - Employers may notify employees that unnamed individuals may be infected.
  - Employers may ask employees for information about travel and infection symptoms.
  - Employers may disclose employee health data to authorities.

## Conclusion

As the COVID-19 crisis rapid unfolds, the response from regulators will continue apace. In both Europe and the United States, data protection laws still apply amid this global health crisis. While regulators have emphasized there is now some flexibility, the basic requirements hold. Organizations should stay attuned to updates from the authorities and err on the side of minimizing data use and collection where possible.

---

### *About NetDiligence®*

*NetDiligence® specializes in Cyber Risk Readiness & Response services. With more than 18 years of experience in cyber, NetDiligence is an award-winning provider of innovative cyber risk management software and services to the insurance industry, including QuietAudit® Cyber Risk Assessments, the eRiskHub® cyber risk management portal, and Breach Plan Connect® software-as-a-service (SaaS) and paired mobile app to help policyholders with data breach response planning. NetDiligence publishes an annual Cyber Claims Study and hosts annual Cyber Risk Summits in Philadelphia, Santa Monica, Toronto, London, and Bermuda. For more information, visit <https://netdiligence.com>.*