Baker McKenzie.

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Strategies for Managing Employee Privacy in a Post-COVID World

ACC NCR | July 27, 2021

Housekeeping

This session is being recorded.

If you have a Question, please put it in the Q&A box and the panel will try to answer. If we don't get to your question during the program, we will follow up after.

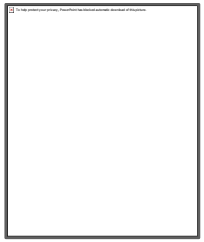
Slides and the recording of today's session is available on the ACC Website at: ACC NCR Program Archives .

CLE Forms will be emailed to you after the program.

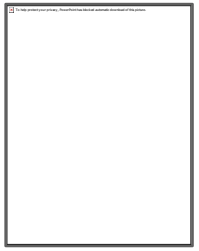
Speakers

Krissy Katzenstein
Baker McKenzie
Krissy.Katzenstein@
bakermckenzie.com

Michael Egan
Baker McKenzie
Michael.Egan@
bakermckenzie.com



Mike Kallens
Nasdaq
Michael.Kallens@
nasdaq.com



Karen Moore
Unisys
Karen.Moore@
unisys.com

Agenda

1. Workplace vaccination programs
2. Managing a remote workforce
3. Monitoring and tracking increased employee data
4. Addressing employee privacy from a global perspective

1

Workplace vaccination programs

Workplace vaccination programs

Mandate vaccinations? Or "strongly encourage"?

- EEOC permits employers to require vaccines if justified by health risks to other employees (with exceptions based on disability and religious reasons).
- Some states have passed or have proposed legislation prohibiting vaccine requirements, differential treatment of persons based on vaccine status, or prohibiting inquiries into vaccination status
    - Kentucky's new law gives every person the right to decline immunization
    - Montana's new law directly prohibits treating customers, patrons, employees, or other persons differently because they are or are not vaccinated, or discriminating against them in connection with the terms and conditions of employment or provision of services
    - Maryland and Virginia both have pending legislation (but tabled)
- Many companies are strongly encouraging employees to get vaccinated

Workplace vaccination programs

Proof of vaccination

- Per EEOC guidance, employers can ask employees if they have received the vaccine or ask for proof of vaccination. To avoid issues under the ADA and GINA, employees should answer “yes” or “no” only.
- Communication to employees must be clear:
  - Provide a GINA safe harbor disclosure when asking about vaccination status
  - Communicate to employees that the employer will consider and attempt to accommodate disabilities and sincerely held religious beliefs
  - Modify point of collection notices to explain that the company is collecting inoculation information about employees and the purposes for which the information will be used
- CDC vaccine cards or printouts from authorities can be “proof”

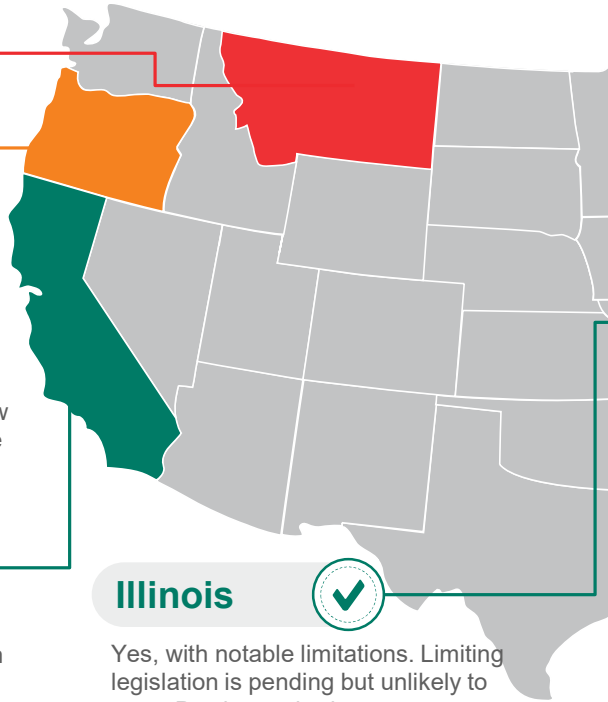
Workplace vaccination programs

Proof of vaccination

- There are several states with current or pending legislation to prohibit employers from asking for proof of vaccination or inquiring about vaccination status, so check applicable state law
- EEOC takes the position that any documents reflecting employee vaccination status are medical records that must be maintained in accordance with ADA requirements
  - Must be kept confidential
  - Must be maintained separately from personnel files
  - Must be kept for one year from the date of the making of the record
- Self-attestation may be a “workaround”
- HIPAA generally will not apply to the collection of vaccination status information from employees, at least *vis a vis* the employer

Vaccines in the US

Can employer require employees to be vaccinated before entering premises?



Montana

No. HB 702 bars employers from requiring employees to receive vaccines "whose use is allowed under emergency use authorization or any vaccine undergoing safety trials."

Oregon

Generally yes, with federal law limitations. No for "health care workers." Limiting legislation is pending.

California

Generally yes, with notable limitations. Limiting legislation is pending but is unlikely to pass. Pay is required.

Illinois

Yes, with notable limitations. Limiting legislation is pending but unlikely to pass. Pay is required.

New York

Yes while the pandemic is severe, but with exceptions noted for federal law. Limiting legislation is pending but unlikely to pass.

District of Columbia

Yes, with limitations.

Kentucky

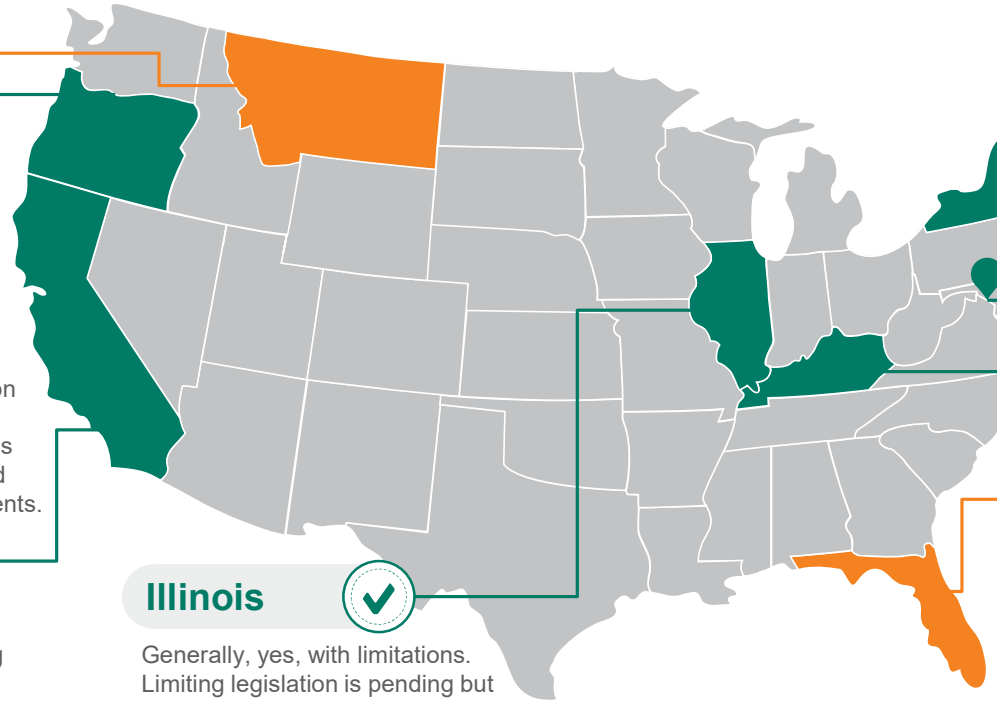
Yes, with limitations. SB 8 provides exemptions from mandatory immunization for individuals who submit a written sworn statement objecting to immunization based on conscientiously held beliefs.

Florida

Yes, with limitations.

Vaccines in the US

Can employer request / require employees to disclose their vaccine status?



Montana

Generally can request disclosure, with limitations. Requiring disclosure is prohibited pursuant to HB 702.

Oregon

Yes. Oregon requires employers to verify vaccination status of employees/visitors before they enter the premises if discontinuing with mask and physical distancing requirements.

California

Yes, with notable limitations. Limiting legislation is pending but unlikely to pass.

Illinois

Generally, yes, with limitations. Limiting legislation is pending but unlikely to pass.

New York

Yes, with limitations. Limiting legislation is pending but unlikely to pass.

District of Columbia

Generally, yes, with limitations.

Kentucky

Yes, with limitations.

Florida

Probably. Executive Order 2021-81 prohibits businesses from requiring patrons/customers to provide certification of vaccination, but it does not appear on its face to regulate the employment relationship.

Vaccines outside of the US

Other key jurisdictions	Can Employer Require Vaccination?	Can Employer Compel Employee to Disclose Vaccination Status?	Can Employer Request Employee to Disclose Vaccination Status?	Data Privacy Considerations
Europe (generally)	✗	✗	✗	vaccination status is **sensitive data** under the GDPR, which requires a legal basis to process (likely lacking)
China (PRC)	✗	✗	✓	Tracking vaccination status considered processing of personal data and requires **informed consent**
Japan	✗ But can restrict access to premises for unvaccinated employees	✗	✓	**Informed consent** and **data security measures** would be required
Brazil	✓ Supreme Court has ruled that mandatory vaccination is permitted; but vaccine supplies are limited	✓	✓	

Workforce vaccination programs

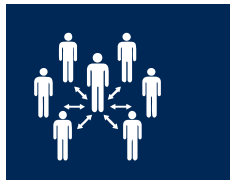
Practical tips

- **Understand the law where you operate**: Some may prohibit the collection of vaccination status information, while others may permit or even require it. The law is changing quickly.
- **Read the room**: Even if vaccination status monitoring is permitted, it doesn't necessarily mean you should. Unnecessary or excessive monitoring can lead to reputational harm.
- **Look at the whole picture**: Your approach to employee vaccination should be closely aligned with your remote working / return to work policy. Each affects the other.
- **Have a clear data plan**: If your company will monitor employee vaccination status, understand the applicable privacy and data protection laws and have a compliant plan from the outset. Document informed consent as required. Consider whether data aggregation, minimization or pseudonymization can mitigate obligations.

2

Managing a remote workforce

Continuing remote work policies



Surveys show…

- According to a survey of 209,000 people in 190 countries by **BCG**, 89% of people expect their jobs to be partly remote after the pandemic ends
- According to **Glass Door**, most workers prefer a hybrid approach, with the flexibility to split time between office and remote locations based on what's most productive for their jobs
- According to **McKinsey's Global Institute**, more than 20% of the workforce could work remotely 3-5 days a week as effectively as they could if working from an office
- Many reports and surveys of global workforces show that the vast majority of remote workers have been able to maintain or improve productivity throughout the pandemic

Cybersecurity Considerations

From network security to home security

- Employees should receive refresher training and tips on secure work.
- Remind employees that sharing company information through non-company applications such as personal email accounts, text messaging, etc. is prohibited
- Appropriate encryption should be used
- Transmit substantial amounts of company information only through secured company servers
- Employees should have a secure workspace with reliable connectivity (not local café).
- Employees should be required to connect to VPN first
- Conversations should be secured from eavesdropping (not in the range of virtual assistants or other IoT listening devices such as Alexa, GoogleHome, etc.)
- Keep work devices secure. Require the employee to agree that no family members or others will access company issued work devices or personal devices used for work.
- Keep physical workspaces secure. Require employees to include elements of traditional security to the home office (locked cabinets, locked desk drawers, passwords, remove IoT devices).
- Consider providing/reimbursing for equipment needed to ensure security (filing cabinets, separate printers, shredder).

Remote workforce privacy considerations

Permanent remote workers

Consider:	
Handling of trade secrets How they should be labeled, where they should be maintained, which employee groups will have access to them, what procedures will be implemented to ensure their security.	**Handling of sensitive hard copy documents** Prohibit the printing or copying of significant company materials without express authorization, or requiring telework employees to keep all hard-copy materials in a locked cabinet when not using them.
Confidentiality/Non-Disclosure If employees will have access to trade secrets/confidential information, be sure to include confidentiality and non-disclosure provisions.	**Outline the company's responsibilities** Any technical support provided to the employee; work expenses the employer reimburses; and equipment the employer provides and repairs (computers, cell phones, teleconferencing equipment, facsimile equipment, anti-virus software, office supplies).
Remote access and authorization Make sure you develop protocols in the policy for remote access to company databases. Ensure that only authorized users have access to your network.	**Distribution and signature** Require teleworking employees to sign (even e-sign) the policy before granting remote access to confidential information. This may be an opportunity to include requisite Defend Trade Secrets Act language.

Remote workforce privacy considerations

Hybrid workers

Consider:	
Concerns for employees working from home and employees returning to the workplace both apply Because hybrid employees are frequently in both places (home and the worksite), both sets of considerations apply.	**Working from a personal device** Confidential information could be obtained by hackers or lost because of lack of appropriate backup.
Accessing company data on multiple devices/from multiple locations Employees logging on from home and from work can open up the company to more cybersecurity risks. Employees should be required to follow company IT policy and use secure connections (VPN, etc.).	**Use of flash drives** Employees may be tempted to use flash drives to store information for ease of use between home and the workplace, but flash drives can be lost and are vulnerable to hacking.
Working from the local drive Employees may be tempted to save files on a local drive on a machine they're carrying back and forth to work (especially if it takes awhile to log onto the company's secure network), making sensitive company information vulnerable.	**Carrying trade secret/confidential hard copies** Employees working between home and the worksite may be tempted to carry hard copy files back and forth, risking lost or misplaced confidential documents.

Remote monitoring of employees

Legal Issues:	Operational Issues:
Make sure to comply with your jurisdiction's rules Monitoring what's on an employee's computer screen, internet activity, e-mails, etc. on devices owned by the employer during work hours is fine in many states BUT check your jurisdiction.	**Be proportionate** Keep it limited to the purpose (such as to maintain the integrity of hardware/software from malicious cyber activity or to protect trade secrets). Don't step over the line into an invasion of privacy.
Provide notices to employees Employees should be provided with clear notices that they're being monitored. Monitoring of employees in general is subject to high requirements due to intrusiveness and impact on employee's privacy	**Protect data obtained** Protect any information you've obtained regarding employee behavior and use it only for the purpose for which it was obtained.
Obtain consent If it's an employee-owned device, make sure you have proper consent from the employee to allow the use of their device for monitoring. Be aware of restrictions on validity of employee consent outside of the US.	**Use passwords for monitoring** Make your databases containing company information password-protected, with each employee using a unique password that he or she is prohibited from sharing with others. This will enable you to monitor your employees' access to company information and flag suspicious activity like mass downloading or sharing.

3

Monitoring and tracking increased employee data

Transferring & Consolidating Global Employee Data

Understand and address privacy regulatory issues

Notice and consent requirements

- Privacy laws may require that employees be notified that their personal data is transferred to third countries
- Certain jurisdictions may require employee consent to transfer their data to third countries
- Certain categories of personal data may be subject to additional transfer restrictions

Data Transfer Restrictions

- European Union and other jurisdictions are placing increasing requirements on organizations transferring personal data to third countries
- Schrems II transfer impact assessments

Data localization requirements

- Requirements in Russia and other countries require certain data be kept in-country

Collecting and documenting diversity data

Mitigate risks and pitfalls in privacy

Develop a cohesive strategy around privilege and confidentiality.

- Collected employee information regarding race/class/gender or other protected categories should be stored outside of employee's personnel file
- If legal is involved/copied on the documents/emails, there is greater flexibility in terms of the content since those documents are likely protected by the attorney-client privilege (assuming the counsel is being engaged for purposes of providing legal advice)
- Ensure only an extremely limited group of individuals at the company have access to the data

Determine what diversity information the company needs and whether it can be lawfully and successfully collected.

- Don't collect more than you need, and it's best to use anonymized data if possible
- There are various issues associated with collecting diversity and inclusion information outside of the US
- Gender data can generally be collected in and outside of the US
- There can also be an issue with having insufficient data (e.g., a company has the race of only 30% of its employees) and making decisions off of it

Monitoring employee social media

General considerations

- Employers generally have more leeway to monitor social media activity on the employer's systems when the monitoring is pursuant to the employer's written policy
- The social media policy should be clear that employees are not entitled to make statements about the company that are egregiously offensive or publicly disparage the company (or otherwise violate the company's code of conduct)
  - Reiterate the company's discrimination and harassment policies, and emphasize that discrimination and harassment on social media is prohibited
  - Racial slurs, sexist remarks, other derogatory remarks that impact a protected class could subject the employer to liability. Employees found to have used such remarks should be disciplined, up to and including termination.
  - Employers should always apply social media policies (and all other policies) in a consistent and non-discriminatory manner

Monitoring employee social media

Employee privacy considerations

- There are some restrictions on employers' ability to monitor or discipline employees for their social media use
- Employers should exercise caution before accessing employees' social media accounts without the employees' authorization or coercing employees to turn over information posted on social media
  - For instance, the Stored Communications Act protects the privacy of wire, oral and electronic forms of communications (including telephone, email and internet communications) from unauthorized access
  - In more than two dozen states, employers are prohibited from requesting social media usernames and passwords from employees. However, many of these states allow employers to request this information to access an employer-owned device or account
- There are federal and state statutes that also regulate an employer's ability to monitor employee social media activity

4

Addressing employee privacy from a global perspective

Employee privacy considerations checklist

What to think about when collecting/processing employee data

- ✓ **Informed consent**: Have employees been notified of the existence and purpose of the data collection and processing? If necessary, have employees given consent, and has this consent been documented?
- ✓ **Proportionality**: Is the data collection proportional to the purpose for which it's being used? Data aggregation, anonymization, and minimization may mitigate an employer's exposure to data privacy liability—consider whether these principles can be applied while preserving the adequacy of the data for the specific purpose.
- ✓ **Legal basis**: Some jurisdictions require that an employer have a legal basis to collect personal information. If such restrictions apply, ensure that such a basis exists.
- ✓ **Data transfers**: If employee data is to be transferred between sites, are specific data transfer mechanisms required (especially in light of Schrems II)? Are appropriate terms in place with vendors and other third parties handling the data? Do data localization regimes restrict the transfer of data outside the jurisdiction?
- ✓ **Data security:** Ensure that any data collected is stored securely and ensure that access is strictly limited to those who require the information. Adopt particular security measures for sensitive data such as health or diversity data and understand whether specific security measures are mandated by law for such special categories.

Questions

Speakers

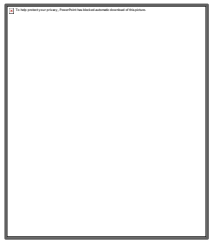
Krissy Katzenstein
Krissy.Katzenstein@
bakermckenzie.com

Krissy Katzenstein is a partner in the Employment & Compensation Practice Group in Baker McKenzie's New York office. Krissy represents employers in a wide range of employment disputes, with a focus on class and collective actions involving systemic discrimination as well as federal and state agency investigations of systemic discrimination and harassment claims. Krissy was named a "Rising Star" in Employment Law by Law360 in 2019.

Michael Egan
Michael.Egan@
bakermckenzie.com

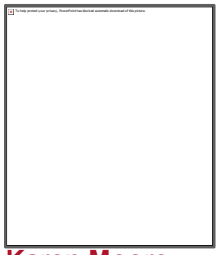
Michael Egan advises clients across various industries, including global online businesses, pharmaceutical companies, healthcare providers, manufacturers, financial institutions, sourcing providers, retail companies, and other organizations regarding the legal aspects of global privacy and data protection, data security, information technology, and related restrictions on data collection and transfer. He focuses on these issues in the context of: global company operations and applications, including websites, mobile and e-commerce applications; data security breach and incident response; transactions; litigation; internal investigations; and government inquiries. He has represented companies before numerous government authorities, including the US Federal Trade Commission, the US Department of Justice and the US Securities and Exchange Commission.

Speakers



Mike Kallens
Michael.Kallens@
nasdaq.com

Mike Kallens is the Associate General Counsel - Ethics and Compliance at Nasdaq. He is a seasoned attorney and executive with 15+ years of in-house legal and management experience focusing on risk management, ethics and compliance, government contracts, contract negotiation and dispute resolution. He has a proven track record of working closely with management to develop and achieve strategic goals, building top performing teams and completing high-risk projects under tight deadlines. Mike is peer-recognized for professional achievements, frequent presenter at national conferences and leader in developing best practices. He was named in 2014 as the Most Outstanding In-house Counsel by the Association of Corporate Counsel – National Capital Region.



Karen Moore
Karen.Moore@
unisys.com

Karen Moore is the Chief Compliance Officer and Privacy Counsel at Unisys Corporation, a global technology service and solutions company (NYSE: UIS). Reporting to the General Counsel and to the Board Audit & Finance and Security & Risk Committees, she is responsible for the design and implementation of the company's global compliance program and charged with oversight of the Unisys cross-functional privacy program. Currently based in the Washington DC metro area, Mrs. Moore has also lived and worked in Moscow, Russia, and Lausanne, Switzerland.

Baker McKenzie.

Resources

Global Privacy Handbook

This annual resource is the collaborative effort of our specialized privacy colleagues throughout Baker McKenzie globally. The recently released and expanded 2020 edition addresses the escalating risks associated with the implementation and management of global databases, increasing outsourcing and transactional issues, litigation, internal investigation and crisis management concerns, all of which can trigger a variety of privacy compliance issues. We offer this handbook to our clients free of charge, upon request.

Connect on Tech

Connect on Tech is our blog and podcast series covering a broad range of topics such as data privacy and security, digital innovation and transformation, AI and machine learning, and other topics related to disruptive technology. The podcast features 10 minute interviews with Baker McKenzie attorneys across the globe to discuss practical tips and the impact of data and technology on business. Visit www.connectontech.com to subscribe to the blog and find our podcast episodes. Alternatively, find the podcast on your podcast player of choice.

Privacy News Roundup

Our Privacy News Roundup is a weekly compilation of data privacy and security news aimed at helping busy privacy professionals stay on top of data-related trends and developments in key jurisdictions around the world.

Baker McKenzie.

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

bakermckenzie.com