COMPLIANCE WEEK

{CYBER-SECURITY}

Cyber-Risk Summit: 7 best practices for protecting employee health data

BY JACLYN JAEGER

Companies whose employees are starting to return to the workplace must ensure they don't unwittingly expose themselves to compliance failures for breaching data privacy and data security laws while simultaneously trying to comply with social distancing and other pandemic-related government regulations and guidelines.

On Thursday, during Compliance Week's virtual Cyber-Risk and Data Privacy Summit, a panel of experts shared best practices as they relate to the complexities facing today's workplace—remote working, health declarations, thermal screening, contact tracing, etc. Among the many relevant privacy and security laws that legal, compliance, and human resources departments must keep in mind in this era of COVID-19 are the Americans with Disabilities Act (ADA), the California Consumer Privacy Act (CCPA), the EU's General Data Protection Regulation (GDPR), and more.

"A lot of this information employers haven't been collecting in the past," said Cynthia Cole, special counsel at law firm Baker Botts. "They don't have a procedure or protocol in place with respect to how they're collecting it. It's new information that employers have avoided collecting for obvious reasons, and now you're in a position where you must do it."

That speaks to the importance of companies reviewing and enhance their current data security and data privacy compliance policies and procedures. Specifically, legal and compliance teams should consider the following seven best practices:

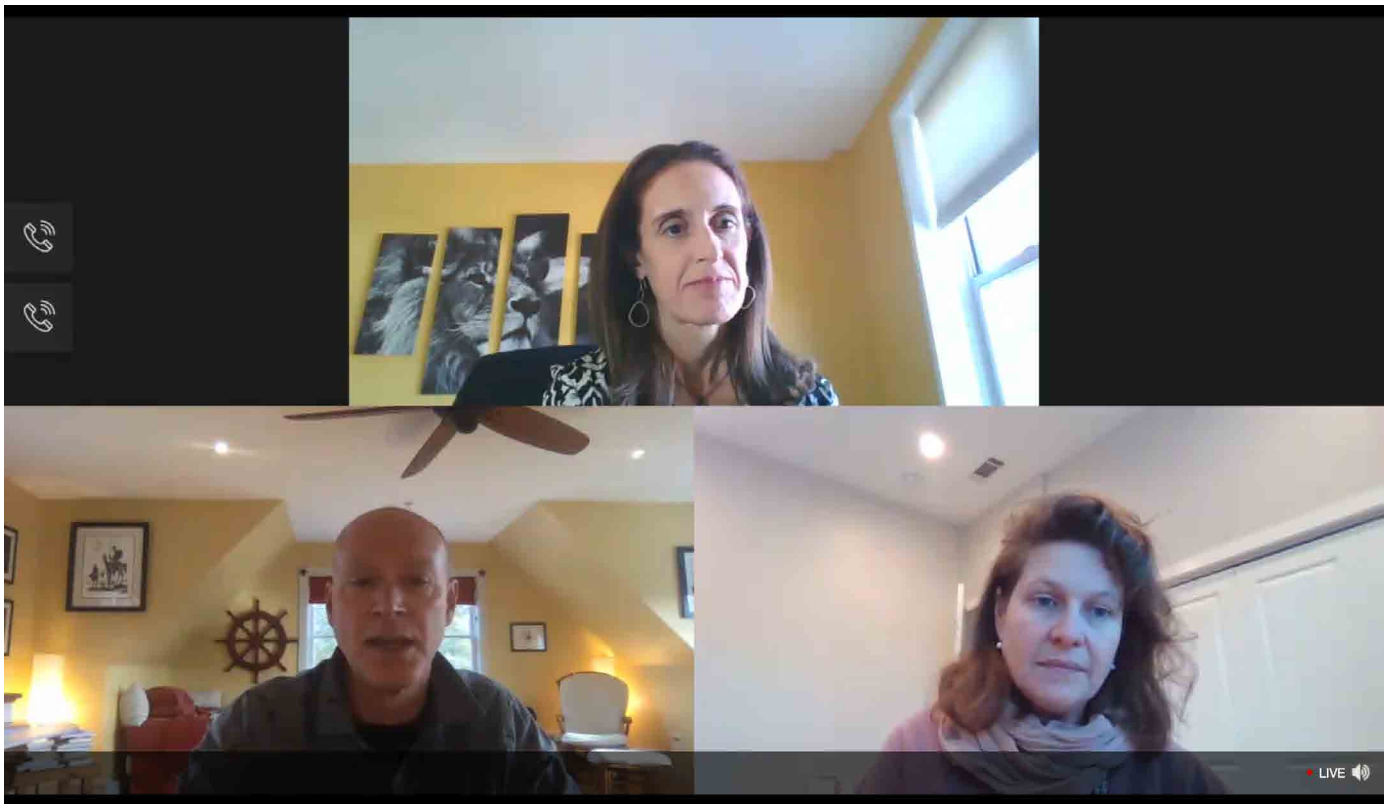
Develop protocols for identifying and responding to high-risk or noncompliant individuals. Not all individuals are going to be accepting of having their temperature taken before entering the workplace, for example. Be prepared for how to respond to circumstances like that, advised Cole. How should employees responsible for that task handle that situation?

Know employees' rights. In the same vein, it's important to keep in mind that employers cannot under law subject certain employees—such as older workers and those with underlying health conditions—to enhanced scrutiny as it relates to health checks. In fact, that can implicate the prohibition on discrimination under the Age Discrimination in Employment Act. If you feel you have a subjective reason to conduct enhanced scrutiny of an employee—someone who is exhibiting signs of illness, for example—"you're going to want to document the living daylight out of it," said Erik Peters, an attorney at Kelly, Remmel & Zimmerman.

Implement or update data privacy and data security policies and procedures. How are you as a company rolling out your data security program and making sure everyone is adhering to the same protocols, particularly in a remote work setting? And how are you able to control, or at least monitor, that employees are abiding by those protocols so that you're able to flag and address potential issues?

Train employees on data security protocols. "Do you have a continuous training program with respect to data security for employees?" Cole asked. If you've been relying on annual check-the-box training, she recommended it be updated and that you put in place real-time testing and ways to actively engage employees about data security protocols.

Limit access of personal data to screened personnel. "Who has access to it internally and externally?" Cole asked. Health declarations should not be available to a wide audience. They should be accessible only to those who have been properly trained on handling personal information, she said. "Are you acknowledging and recognizing who it is that has access in your organization to that personal information and training them specifically on the laws and principles that apply?" Cole added. "That is very important."



Compliance Week's Julie DiMauro (top) moderated Thursday's discussion with attorneys Erik Peters (left) and Cynthia Cole (right) on protecting employee data.

Practice basic data security and data privacy hygiene. Consider employing anonymization or pseudonymization techniques with respect to data, Cole recommended. Pseudonymization means stripping personally identifiable characteristics from the data and replacing it with one or more artificial identifiers, or pseudonyms.

Adhere to rigorous data minimization principles. Data retention policies and procedures should also be considered. If you do not currently have a data retention policy, "you better put one in place very quickly," Cole said.

Regarding the collection of individuals' personal health information, it's important to keep in mind what purpose it serves. "Why is it that you're collecting the information?" Cole said. "That will inform what you do with it and who has access to it. Only collect what is absolutely necessary to effectuate the purpose you're trying to serve." If there is no legal or financial reason to hold on to personally identifiable information, destroy it as soon as it's no longer needed.

The overlay of legal, compliance, and ethical consideration in the world we're living in right now is "mind-blowing," Cole said. To expect a one-person HR department to address and deal with these issues isn't realistic but rather requires having outside counsel and key decision-makers involved, talking about, and working through these issues on a continuous basis, she said. "The price you pay on the front end to get ahead of these issues or at least make a good-faith effort to stem the tide of bad decisions is well worth it." ■