Conducting Remote Workplace Investigations: Challenges And Top 10 Practical Solutions

Insights
1.29.21

As many workplaces have shifted to remote work arrangements, human resources personnel, in-house lawyers, and other workplace investigators are conducting more remote workplace investigations. Remote investigations may involve investigators working remotely, interviewing remote witnesses, or both. These investigations present numerous challenges for investigators and require maintaining a delicate balance between conducting a thorough investigation, protecting employee privacy rights, and ensuring the confidentiality and security of information shared and received by investigators.

Some of the biggest remote investigation challenges are addressed below, including the top 10 practical steps investigators can take to address them.

Challenges Faced By Remote Investigations

Investigators conducting remote investigations face a number of legal requirements, practical considerations, and challenges in ensuring the privacy of employee personal information and the confidentiality of information gathered or shared during an investigation.

Statutory Privacy Considerations

As an initial matter, employers have legal obligations to keep certain employee information private. For example, the Americans with Disabilities Act (ADA), the Health Insurance Portability and Accountability Act (HIPAA), and the Genetic Information Nondiscrimination Act (GINA) all contain requirements to keep certain employee medical information private.

Employers also have legal obligations to protect against the unauthorized release of employees' Personally Identifiable Information (PII). Courts have recognized an employer's duty to protect employees' PII and imposed liability where that duty is breached. Investigators therefore must be careful to protect PII in the course of their investigations.

Confidentiality Concerns

At the same time, for legal and practical reasons, remote investigators must keep investigative records confidential. First, limiting access to investigative documents minimizes claim and litigation

risk. Second, maintaining confidential investigative records and communications is important for preserving attorney-client privilege and work product when counsel is consulted, or the investigation is directed by counsel. Third, investigators must maintain the confidentiality of certain business information pursuant to company confidential information policies. Finally, maintaining the confidentiality of information shared during an investigation to the extent possible encourages employees and other witnesses to be forthcoming and honest.

WFH Leads To A New Slate Of Challenges

Maintaining employee privacy and data confidentiality during a remote investigation, however, is particularly challenging. An investigator working from home may not have a separate, confidential space in which to work. The investigator could inadvertently discuss sensitive or personal matters in the presence of others in the household. Printing and disposing of documents containing personal employee information in the household trash, saving sensitive information to a personal device, emailing it to a personal email account for remote use, or simply leaving confidential documents lying around in the house may also result in inadvertent disclosure of private or confidential information.

Investigators who conduct interviews in public spaces, such as on Zoom or telephone calls made at a coffee shop, also risk exposing private or confidential information. Others in the shop may overhear the investigator's discussion with a witness. Using the coffee shop's public wifi system could also allow others to access that information.

Remote Witnesses Present Yet Another Hurdle

Interviewing remote witnesses also poses challenges. Other individuals who are unconnected to the investigation may be in the room but unseen by the investigator. Those individuals might overhear the investigative interview or see sensitive documents shared during the investigation. They could also document or record the interview for a variety of reasons, including use in future litigation or to share information from the interview with others.

Digital-Age Video Concerns

Finally, use of videoconference technology also raises potential issues. Open windows on computers during a videoconference call could inadvertently expose private or confidential information. Videoconference technology also creates the potential that personal or confidential information is mistakenly shared on a screen.

Top 10 Recommendations

How can an investigator best protect private and confidential information during a remote investigation? Consider these 10 recommended guidelines:

1. Establish a private, closed space in your home to conduct witness interviews where you cannot be overheard or interrupted by others.
2. Ask your witnesses to set up in a private, closed space as well, and before beginning the interview ask the witness to confirm that they are in a private area with no one else present or within earshot.
3. Advise the witness up front that you do not consent to allowing the witness to record the interview (see below for obtaining the witness' consent for you to record).
4. Prior to starting a videoconference interview, advise the interviewee to clear any sensitive information and to close sensitive applications from their screens.
5. If it is necessary to use hard copies of investigative documents and files while working remotely, maintain them in one secure area in your home office or work space, ideally in a locked file cabinet.
6. Do not dispose of any investigative documents in the household trash or recycling. Instead, return documents to your worksite for secure disposal or use a disposal service specifically designed for securely disposing of confidential documents.
7. Avoid using personal devices and email accounts to send, receive, or store information.
8. Avoid conducting investigative interviews in public areas.
9. Do not use a public wifi system to conduct interviews or otherwise perform other tasks related to the investigation such as emailing.
10. If a videoconference concerns attorney-client privileged matters, counsel should state up front that the meeting is privileged and remind participants not to create separate electronic conversations (texts, chats, etc.) regarding the meeting.

Recording Remote Interviews

The proliferation of teleconferencing tools such as Zoom, Microsoft Teams, and others has made conducting remote workplace investigations much easier. These technologies offer options for easily recording interviews, but should an investigator do so?

Recording remote interviews can be risky, particularly without obtaining the consent of the interviewee. Most states only require the consent of a single party to a recording. However, fifteen states require both (or all) parties to a conversation to consent to recording it. Those states include California, Connecticut, Delaware, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Oregon, Pennsylvania, Vermont, and Washington. In these states, investigators should obtain an interviewee's express consent before recording a call or videoconference session. Notably, penalties for violating state statutes can include civil penalties as well as criminal liability.

Even assuming the witness consents to recording, investigators should consider whether it's a good idea to record interviews. A key consideration is whether the recording would be discoverable in any litigation or other proceeding, or perhaps would be subject to production to government investigators such as the Equal Employment Opportunity Commission, Department of Labor, and others. There can be benefits and drawbacks to producing the recordings. Investigators should carefully consider whether recording interviews is the best approach in each case and with each witness. Particularly when a matter is more likely to wind up in litigation, investigators should consult with counsel about the pros and cons of recording remote interviews.

How can investigators ensure that remote interviews are properly and lawfully recorded?

1. Know the applicable law for obtaining consent before recording an interview and if you're not sure, consult with counsel.
2. Create a plan for how to inform the interviewee that the interview will be recorded.
3. Obtain written consent to record from the interviewee in advance.
4. Know the recording functionality of the video platform you're using and use the consent function where available. For example, on Zoom, a call can be set to require all participants to consent to recording before they join a meeting.
5. Announce at the beginning of an interview that it will be recorded, that the participant has consented, and that participation constitutes further consent to record.

Information Security

Data security is a big issue in workplaces generally and an important consideration in remote workplace investigations. As an initial matter, investigators should ensure that they are conducting remote investigations using secure technology. If using Zoom, for example, review the security settings and be sure to use the most secure methods possible (including password-protecting meetings, enabling the "private meeting" setting, and disabling screen sharing for participants and private chat).

Additionally, avoid using consumer shared drives to share sensitive documents and information. It's best to use a secure data sharing platform, which should include end-to-end encryption to prevent third parties from accessing shared data.

Securely sharing company documents for a remote interview also presents confidentiality challenges. Potential options include sharing documents on the screen during a videoconference, sending hard copies of the documents just before the interview, or using a secure file sharing system such as a virtual data room. None of these options is foolproof. Whatever method an investigator chooses, investigators should require witnesses to sign a non-disclosure agreement prior to the interview, which should include provisions prohibiting reproduction of documents, use of

data or documents for any purpose other than the interview, and requiring return of all hard copy documents, if applicable.

Smart speakers are another hot button issue in remote investigations. Investigators may have smart speakers such as Alexa and Siri in their homes or on their phones. These smart speakers record verbal communications, which are analyzed by the companies who sell them to improve their artificial intelligence capabilities. Investigators therefore need to be particularly careful about ensuring that they are not within earshot of smart speakers when conducting remote investigations.

Finally, investigators should be aware of and follow appropriate data preservation and storage protocols. Conducting remote investigations creates new challenges in the data security realm, as investigators need to ensure that sensitive and confidential data collected is properly managed. Employers should update data storage and retention policies to ensure that remote investigators have proper guidance on data storage.

What are some best practices for ensuring information security in remote investigations?

1. Study the technology you plan to use and make sure security settings are properly set prior to each witness interview.
2. Carefully consider how you will share documents that contain confidential or sensitive information and use a secure approach.
3. Require witnesses to sign non-disclosure agreements prior to interviewing them.
4. Turn off your smart speakers!
5. Update and follow data preservation and storage policies.

Remote investigations are convenient, efficient, and likely are here to stay. They present numerous privacy, confidentiality and data security challenges, but with proper planning, a remote investigator can ensure compliance with applicable laws and business needs.

Service Focus

Privacy and Cyber