BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Pandemic Response

Privacy, Security Issues

A great deal of complexity arises in the context of a dangerous pandemic when collecting and transferring the sensitive health information of employees and visitors. Companies must seek to not only protect employee health and safety, but also undertake appropriate precautions for the handling of the sensitive data about their employees. Companies that fail to consider data privacy and security may find their employees less than willing to provide and exchange important information. This tension between workers and the company may not only endanger health but also undermine shared business continuity objectives.

Privacy Considerations for Pandemic Planning

BY MARGARET P. EISENHAUER AND STANLEY W. CROSLEY

On June 11, 2009, the World Health Organization (WHO) declared a Level 6 H1N1 pandemic.[1] This declaration reflects the uncontained transmission of the H1N1 influenza virus across multiple countries in multiple regions. The pandemic declaration has led governments, communities and organizations to ramp up preparedness efforts as we enter the prime flu season in North America. As companies evaluate their pandemic planning in the context of the current H1N1 outbreak, it is important to consider privacy and information security issues that arise in pandemic response programs.

Many companies have previously adopted comprehensive pandemic preparedness programs. These programs generally assume a high rate of worker infection resulting in a significant impact on the workforce from a global epidemic, including worker absenteeism rates of 15-20 percent of the workforce, stemming from causes such as family-member infection, school closings or loss of public transportation resources. These pandemic preparedness plans are designed to protect employee health and safety by attempting to limit the spread of the disease within the organization as well as

[1] For more information about the current state of global pandemic, please visit the World Health Organization online at http://www.who.int/csr/disease/swineflu/en/.

 ISSN 1538-3423

to enable business continuity for the duration of the outbreak and to minimize the economic impact on the organization.

Unfortunately, most existing corporate pandemic programs were not designed with privacy considerations in mind. This article is designed to help companies evaluate their pandemic response plans through the lens of privacy and security as well as general information risk management and health outcomes management.

Although the H1N1 flu has not yet been very severe, the Level 6 designation has already triggered company efforts to collect employee health information and launch pandemic measures. Health information continues to be some of the most sensitive information about individuals that companies process, and the emotional context of processing the information during a period of crisis adds complexity. The processing of health-related information is also highly regulated by U.S. and international laws.

Pandemic Program Elements

To manage privacy in pandemic programs, we must first consider the privacy issues that arise during the stages of pandemic response. Corporate pandemic programs generally contain four key elements: (1) screening, (2) cleaning, (3) social distancing, and (4) quarantine. The goals for each element are reasonably clear, but the privacy and security considerations vary on the steps taken to achieve the goals.

Screening

The first key element of pandemic response is screening for influenza to identity specific individuals that have symptoms of flu or are otherwise at high-risk of contracting flu. Companies may also wish to identify workers that are at high-risk of complications from flu, due to other health characteristics such as pregnancy or generally weakened immune systems. Screening programs may encompass company workers as well as other individuals that visit the corporate premises.

Screenings are most typically done by the individuals themselves using self-assessment checklists that contain lists of flu symptoms or risk factors. For example, upon entry to the facility, individuals could be asked to review the assessment checklist and verify that they are feeling well and do not have the symptoms on the checklist. They may also be asked to certify that they have not been exposed to known instances of the flu. Additionally, some organizations may ask individuals to visit the company health center if they have certain symptoms while at work, such as a fever or sore throat. Some companies also ask managers and supervisors to report symptoms exhibited by their direct reports as well.

While screening may be self-assessed at the individual level, it may also be done in a more centralized location. For example, some companies require individuals to complete, and even sign, screening forms when they enter a facility, while other companies require managers and other workers to report the incidence of disease to a central health data collection repository. The screening process may collect specific health information (such as whether the individual has a sore throat or other symptoms). It may include collection of information via technological means, such as heat sensors to detect fever and risk information (such as whether the individual has been in contact with infected persons or traveled to places where the incidence of flu is known).

Cleaning

The second key component of pandemic planning is cleaning/disinfection. Companies have obtained a wide variety of internal and external (using specialized vendors) cleaning protocols. These protocols include issuance of disinfecting materials (such as hand wipes) to workers, provision to individuals in a facility of surgical masks, and other types of equipment.

Companies that fail to consider data privacy and security may find their employees less than willing to provide and exchange important information. This tension between workers and the company may not only endanger health but also undermine shared business continuity objectives.

Cleaning processes may be supported by corporate efforts to reduce shared surfaces, either by issuing latex gloves or limiting the need for shared surfaces, such as by removing common area telephones or propping open doors. For example, by programming elevators to stop at every floor, you eliminate the need for workers to press elevator buttons.

Cleaning processes generally do not trigger significant privacy concerns, although a cleaning team entering an employee's cubicle to undertake a deep-cleaning is certainly indicative of the health status of the employee occupying the cubicle. The program should be respectful of employees if deep-cleaning services affect the personal spaces within offices or cubicles and cleaning vendors that have broad access to the facility should be credentialed in accordance with standard information security protocols.

Social Distancing

The third component of pandemic planning is social distancing, a collection of controls designed to avoid spread of the virus by limiting in-personal human interactions. Companies generally consider worker-to-worker interactions as well as interactions between company personnel and external parties, such as customers, consumers, patients, suppliers or visitors.

Many companies have already established preferences for teleconferences or video conferences over live meetings as a way to reduce costs. Similarly, companies may have shifted external interactions to phone/web/kiosk as well. Pandemic preparation may provide another incentive to these types of initiatives.

Other social distancing steps may also be necessary. For example, companies may institute travel bans or other prohibitions on attending events in areas where flu is prevalent, cancel non-essential gatherings (such as sales meetings), limit the number of attendees that

  PVLR ISSN 1538-3423

may participate in live meetings or require meetings to be held in rooms where minimum distances can be maintained among the attendees. Common areas, such as cafeterias or gyms, may be closed or maximum capacity levels may be reduced.

Social distancing steps may be taken for the entire workforce or for those employees with higher risk of complications from flu. For example, the company may wish to implement specific steps to isolate workers who are pregnant or generally susceptible to infections. Workers in these categories that deal with the public directly might be moved to call-center operations or assigned to less busy shifts.

Quarantine

The final component of the pandemic planning is quarantine. Employees may be quarantined for a certain period of time during their own illness, and the quarantine may also extend to individuals who have been exposed to the virus but are not themselves ill. For example, individuals whose children have the disease or where the disease is otherwise present in the household may also be asked to remain on quarantine until the infection has passed.

To manage quarantine, companies may require a tremendous amount of personal information. The information ranges from information about workers, family members and potentially non-family household members (such as roommates) on a diagnosis or symptoms (if a formal diagnosis is not available), date of onset, potential duration of the illness, and complications. Some companies also require documentation of the illness to be provided by a health care professional.

Many companies have determined that they will not engage in the active management of quarantines, but will simply require their workers to verify their health prior to returning to work. In this case, it is likely that the need for data collection is minimized. The pandemic program coordinator should establish a baseline for data collection so that companies can limit their requests to the minimum data needed to document the quarantine event.

Practical Steps for Managing Privacy and Security in Pandemic Programs

As companies refine their pandemic response programs, they need to be sensitive to a number of different elements ranging from legal compliance to communications. The following checklist may provide a helpful reference of privacy and security considerations that should be taken into account:

Identify key resources.

Each company should identify key national and community resources to provide information on the current state of the pandemic and recommended procedures. Information about the flu, including recommendations for cleaning, social distancing and quarantine, can change rapidly. For example, the Centers for Disease Control and Prevention (CDC), the Department of Health and Human Services (HHS), and other U.S. agencies regularly publish updates on pandemic response and preparedness at http://www.flu.gov. Extensive information for businesses (including an excellent checklist) can be found at this website.[2]

It is important to have a defined process for learning and implementing new recommendations in real time. Most companies start by designating a pandemic planning coordinator to oversee the program and program revisions. To the extent that the company needs to establish relationships with government agencies and non-government organizations to ensure timely access to information, those should be established as soon as possible.

Communications program

Just as the company has to process information in real time, it must also effectively communicate with all workers as the pandemic develops. If the flu becomes more severe and the mortality rate rises, workers will likely feel panic and other strong emotions. By providing regular and appropriate communications, the companies can reassure workers and provide support for workers as they address the individual emotional toll that the disease may have.

If you use data collection technology, such as heat scanners, ensure that individuals understand what the technology does and how the data collected will be used and maintained. Ensure that operators are prepared to answer expected privacy and security questions.

Employee incentives

The communications program should also consider how to reduce conflicting messages that employees may received. For example, if the company wants to ensure that employees follow quarantine requirements when a household member has flu, the company should refrain from withholding pay during quarantine period. Instead, either provide remote work opportunities or else consider paid leave programs. Similarly, if you want employees to self-report flu symptoms, you have to ensure that they will not be sent home without pay upon making a report. As the flu develops, companies will want to find creative ways to ensure that employees are appropriately incented for caution and candor with regard to pandemic planning.

Data collection

Consider both the nature of the data collected for pandemic planning purposes and the source. What data do you really need? Your workers are likely the best source of information about themselves and their households with regard to influenza. If possible, avoid having data on individuals collected by other workers, particularly if those workers are not trained appropriately.

[2] See the checklist at http://www.flu.gov/professional/pdf/businesschecklist.pdf.

If you use data collection forms, such as self-screening forms, assess whether you actually need to collect the forms or whether you simply want to use them as a formal means of drawing the individual's attention to the symptoms they should be checking. If collection of the forms is deemed important, try to collect the minimum data necessary. For example, workers should not be asked to provide Social Security numbers on these forms.

If you use data collection technology, such as heat scanners, ensure that individuals understand what the technology does and how the data collected will be used and maintained. Ensure that operators are prepared to answer expected privacy and security questions.

Companies may also need information for business continuity purposes that is unrelated to health. Companies may need to conduct a skill survey to understand skills generally across the workforce, so that individuals who are not ill can be assigned to tasks performed by people who are absent. For example, understanding which workers speak Spanish may enable a company to offset absences in its consumer call center. Each company should consider if (or when) these types of datasets can be used post-pandemic.

Understand the law

The collection and use of health information is highly regulated by U.S. and international laws. In addition to privacy and data protection laws, companies must consider applicable labor and employment laws, the Americans with Disabilities Act, and anti-discrimination laws.

For individuals in Europe and other countries with comprehensive data protection laws, companies should be careful to comply with all the requirements related to ''special categories of data,'' including registration of data processing activities and authorization for any data transfers.

For all international data processing, companies must consider the proportionality test. Proportionality suggests that in the instance of a serious pandemic, more aggressive processing of information would be legitimate under the law than would be permissible in normal times. However, a pandemic is not a blanket license to process sensitive information. Given the moderate severity of the flu so far, only a small amount of sensitive information processing may be justified. Additionally, even if the flu becomes severe, it is unlikely to be the case that health information can be processed without notice and some level of choice. As a practical matter, many countries will require companies to obtain affirmative consent from workers prior to processing any health-related information for pandemic management.

In the United States, several state security and security breach notification laws apply to health information. For example, if computerized personal information relating to an individual's health is exposed to an unauthorized third party, companies will have obligations to send breach notification letters in California, Texas, Arkansas and other states.

Additionally, if employee health services professionals are subject to the Health Insurance Portability and Accountability Act Privacy Rule and Security Rule, steps must be taken to ensure ongoing compliance with the HIPAA requirements. Even inadvertent disclosures of protected health information may trigger the new HIPAA breach notification rules and have serious consequences for the company.

Companies should also consider their collective bargaining agreements and works councils. If workers may need to be reassigned as part of a business continuity program or to achieve social distancing objectives, the company may need to seek approval for the program. It is strongly advisable to consult with your workers' representatives in advance, so that they have time to consider the measures you may ultimately want to take.

Transparency

Companies should develop and publish a privacy statement for the pandemic program to address privacy and security of information collected for pandemic and business continuity purposes. This privacy statement should indicate the types of data that will be collected for pandemic management purposes and business management continuity, as well as the uses and disclosures of that data. If possible, provide assurances to your workers that their personal information will not be used for other purposes, such as job performance evaluation. The goal is to develop trust and ensure that workers have the confidence needed to share sensitive information about themselves.

For all international data processing, companies must consider the proportionality test. Proportionality suggests that in the instance of a serious pandemic, more aggressive processing of information would be legitimate under the law than would be permissible in normal times. However, a pandemic is not a blanket license to process sensitive information.

Building trust is especially important if you need to collect information about flu risks for business continuity planning. For example, it may be essential to know which employees are pregnant or have other perhaps more stigmatizing conditions (such as HIV) so they can be prioritized for remote work. But an employee may not wish to disclose that information because she is awaiting a promotion or has applied for a new post. Providing assurances that risk factors will be not be used for any other purposes may give the employee confidence to share the critical information with the company.

Of course, the privacy statement must accurately reflect actual practice. Controls should be instituted so that the pandemic program data is secured appropriately, accessed only by authorized individuals with a need-to-know, used only for the purposes described in the privacy statement, and retained only as long as needed or otherwise in accordance with the company's document retention program and then appropriately destroyed at the end of the retention period. This will be

  PVLR ISSN 1538-3423

particularly important in countries with comprehensive privacy and data protection laws.

Data-neutral steps

Where possible, organizations should take steps for pandemic planning that are individual information neutral. For example, cleaning protocols, distribution of supplies, travel bans and so forth may be implemented without the need to collect information from or otherwise target individual workers. Companies may wish to simply apply protocols across entire business units, offices, or departments, rather than single out individual workers for treatment under the pandemic plan.

Remote work

As part of the business continuity planning process, companies should seek to identify all functions within the organization that can be performed from a remote location, such as an employee's home. Efforts can then be made to identify the equipment and facilities needed to enable remote work. These may include issuance of laptop computers or other devices or implementation of collaboration tools such as social media.

Companies should also consider to what extent access to information that the employee needs to do his or her job is required. Employees that can work from home using remote access technology may be able to do all of their jobs. However, if the company cannot support remote access for a large percentage of its workforce, it may need to make data available to workers on local or portable devices. Encryption and other security controls will have to be expanded in order to ensure that the employees that have access to locally stored data can do so in compliance with corporate security initiatives.

Similarly, companies may want to develop schedules to support remote access. For example, some workers (such as help desk workers) may need continuous remote access to company systems. Other workers, such as individuals in human resources, lawyers, or managers, may need occasional access such as 20 minutes every two hours to download and upload e-mails and files. By developing a matrix showing how remote access resources are allocated, the company can maximize business continuity while also maximizing the ability of individuals to work productively when subject to social distancing or quarantine requirements.

CONCLUSION

The most important goal for all company pandemic plans is clearly to protect the health and safety of its workers. However, a great deal of complexity arises in the context of a dangerous pandemic when the collection and transfer of sensitive health information about employees and visitors may be important to that primary goal. Companies must seek to not only protect employee health and safety, but also undertake appropriate precautions for the handling of the sensitive data about their employees. Companies that fail to consider data privacy and security may find their employees less than willing to provide and exchange important information in the midst of a crisis. This tension between workers and the company may not only endanger health but also undermine shared business continuity objectives.