5 Data Retention Best Practices for Safe Spaces

By Laura Davis-Taylor

As companies scramble to safely reopen, questions abound about what to do with the data collected when screening employees and customers for coronavirus. This data is crucial for protecting those that enter the business, as well as tracing the virus on a city and national level. Unfortunately, there are two sides to this coin, pressure on both sides, and a whole lot of gray area.

On the one hand, there's the social responsibility to keep customers and employees safe, which ties directly into Duty of Care. Not doing so could result in a lawsuit like the one that Smithfield Foods is facing, or a workers comp claim in places like California. On the flip side, there's pressure to maintain the privacy of personal data, aka Protected Personal Information (PPI).

Both sides have advocates backed by strong beliefs. In any given business, the HR, IT and law departments will likely have conflicting priorities about data retention. So how can a business find the balance between social responsibility and privacy rights?

In countries like the U.S., where there's not a single blanketed mandate on the matter (unlike Switzerland), the way forward can be confusing. With information and recommendations changing by the minute, a business's best bet is, quite frankly, to cover its butt. Businesses need to be prepared for anything from an employee lawsuit to a compliance audit.

We're in uncharted territory here, so the best course of action is to be proactive and ultimately be prepared. At the end of the day, it's the business's responsibility (and liability) to keep both individuals and their private data safe and secure. With that in mind, here are five best practices for data retention when creating safe spaces.

1. Keep Data for 21 Days

The data that a business may collect to protect those that enter may include anything from a name, phone number and email address to an image, which may be necessary to monitor the temperature. It's up to the business to decide what to collect — and how long to keep it.

Data will include both the results of Q&A and/or temperature screenings, along with the name of the person that generated the results. Notably, the latter is considered PPI. The recommendation here is to keep all data for 21 days, which more than covers the 14-day window between exposure to the virus and the onset of symptoms.

2. Anonymize Data After 21 Days

So what are you supposed to do with this data after 21 days? The best practice is for businesses to then anonymize the data. That means, keep personal info like names for 21 days only. Beyond that, you'll continue to keep the results data, but it won't be attached to a personal identity.

This will allow you to maintain information that will be helpful for tracking long-term trends, but not specific enough to be used for contact tracing beyond 21 days. It also covers your business in case a mandate comes down that demands access to this information.

3. Be Transparent

Transparency is crucial whenever you're doing any kind of tracing that involves a camera, especially in cases where a camera is used for thermal imaging to detect elevated temperatures. Businesses must tell employees and customers alike exactly what they're doing, and why.

There's no room for omission here, as complete transparency is imperative in order to give individuals a choice. If a customer is uncomfortable with your protocol, they're free to choose not to enter your business. Likewise, if someone in California wants to keep their information private, a business must have the ability to remove their personal information from the platform in compliance with CCPA.

4. Know Local and Regional Mandates

Recommendations on how to conduct health screenings and what to do with the data will vary from city to city, state to state, and from one industry to the next. Guidance may also conflict on a local and regional level, but it's every business's responsibility to know all guidelines and follow them to the best of their ability.

As we know, these recommendations are likely to continue to change and evolve, so you'll need to stay up to date. And in the absence of any guidance on data retention, it's best to cover your bases by following the best practices detailed here.

5. Adopt a Flexible, Secure Platform

The platform you choose to collect and store this data must have the ability to keep all data secure and anonymize PPI data after 21 days. Choose a platform that can tackle both immediate testing needs and longer-term data and tracking concerns. The solution should be capable of being configured to match your specific workflow. Flexibility also includes the ability to configure at both the device and cloud level.

In these uncertain times, we can be sure of one thing: Businesses are accountable for data and policy compliance. Adopt a safe space protocol for data storage to mitigate risks your business may face now, and well into the future.

Our Learning Center is committed to sharing important guidance to help the industry navigate the complexities of the ever-evolving Safe Space landscape. The information shared is informed by experience working with client stakeholders, as well as independent research.

For more on how our Safe Space Solutions can help return confidence to your enterprise Please connect with either Beth Warren [beth.warren@cri.com] Laura Davis Taylor [ldt@inreality.com] for strategy and use cases.

inReality + CreativeRealities