COMMENTARY

Privacy of Staff Biometric Data in Vulnerable Population Outreach

Authors _ Audrey Barbakoff (albarbakoff@kcls.org), Community Engagement and Economic Development Manager at King County Library System. **Rekha Kuver** (rpkuver@kcls.org), Youth and Family Services Manager at King County Library System. **Christine Anderson** (chaanderson@kcls.org), Outreach Services Coordinator for King County Library System.

In restoring Outreach services following COVID-19, Mobile Servcies staff at King County Library System (KCLS) have encountered a growing concern for staff data privacy. A significant number of facilities have begun replacing paper sign-in logs with automated kiosks that record, store, and share a large amount of staff personal, medical, and biometric data. This article provides an example that demonstrates the widespread implications for outreach staff data privacy, and explores broader considerations related to this trend. It shares principles that may assist other libraries in developing guidelines for staff data privacy during outreach visits.

A strange thing happened when King County Library System (KCLS) Mobile Services staff went inside a senior living community for the first time in over a year. The community had replaced its pre-pandemic paper visitor sign-in sheet with an automated kiosk. This seemed reasonable: post-COVID-19, most facilities were now not only logging the visitors to their vulnerable residents, but also asking a few health-related questions and maintaining records for contact tracing. When prompted, the library staff person entered the KCLS department phone number. With only that information, the machine printed a visitor badge—with the full first and last name of a different employee, who had never been to that site. Why did that happen? Both library staff and the front desk facility staff were baffled.

After a few days of research, the department manager found the answer. The company that developed the kiosk had also sold units to other senior living facilities in the area. More than a year ago, a staff person had entered her name and the department phone number into a kiosk at a completely separate, unaffiliated site. Her information was added to the database of a private software company. The company kept the record for all that time, and it shared its entire database with every one of its customers. That customer base appeared to be growing rapidly, as KCLS staff started seeing the kiosks proliferate at many senior living facilities.

Change in Privacy Issues

Before the pandemic, paper sign-in sheets at the front desk had been common. As the residents of group living communities are often members of highly vulnerable populations, signing in seemed like a reasonable safety precaution. Encountering a kiosk pre-pandemic was rare, and it generally asked for nothing more than a name and perhaps a photo.

Post-COVID, the kiosks are configured for much more, and the risks to data privacy have increased exponentially. This technology can collect and record a large amount of personal and medical data from visitors: body temperature and other biometrics, vaccination status, health attestations, and responses to survey questions, associated with photographs or facial scans, phone numbers, and time and place of all previous logins from any participating locations. While a paper visitor log was held locally and likely shredded a short time later, kiosk entries are preserved for an unlimited and unspecified amount of time, accessible from a database available anywhere in the world. This is not merely a change in visitor log technology. It is a radical shift in some basic assumptions about health data privacy for a wide array of visitors, including library staff who visit these communities.

Not only do the kiosks fundamentally change the privacy considerations of the information they collect, they can easily take in new forms of data that previously would not have been collected. Some kiosks use facial recognition. Some can verify vaccination status or COVID test results. One was configured to prompt library staff to record their pulse and blood oxygen saturation. Via the kiosk, a staff person's photograph, full name, phone number, biometrics, and health questionnaire answers are given to a private company, and shared with all the customers of that company, without any obvious restrictions on what they may do with this data or how long they may keep it. In fact, some companies do not have a mechanism by which a person who has given over their information through a kiosk can successfully request that their information be deleted.

An added consideration is the data literacy of senior living facility staff, both those who initially configure the kiosk and the front-desk staff who administer its day-to-day use. In initial setup, some of the most concerning features may be deactivated. Were staff at the facility aware of the options, and what choices did they make? Are front-desk staff aware of these choices and able to answer library staff questions accurately? Are front desk staff empowered to allow KCLS staff to decline to use the kiosk, or to permit an accommodation such as not having their photo taken?

The way these kiosks are marketed discourages such questions. They seem to be generally advertised as a convenience for facility staff—the visitor simply stands in front of the kiosk, and the software handles the rest. The more the software is allowed to draw from and add to its global database of information, the simpler it is for the front desk. This does not promote front-desk staff developing an in-depth understanding of how the kiosk works. Also, invasive features are marketed as safety protections, which encourages staff to keep them enabled even when they do not contribute to residents' health and safety. (Who was made safer by asking library staff to record their blood oxygen levels?)

The Library Response

Different libraries may come to different conclusions about what policies and practices should be put in place to address these privacy concerns as they affect library staff. KCLS has developed a set of guidelines to safeguard staff biometric data privacy while also complying with reasonable health and safety requirements. They are summarized here in the hope that other libraries can proactively consider how to balance these needs before encountering a similar situation. Individual staff members have widely varying personal comfort levels with sharing personal and medical data, so a clear organizational practice is important.

The core principle of the KCLS guidelines is that no outside entity can store a library staff member's name associated with other personal data, including temperature, photo, or other biometrics. This is regardless of format. For example, a paper log that says "Jane Doe, Body Temperature 98.6" is impermissible, as is a kiosk that stores both of these in a single record. Library staff may have their temperature taken before entering a facility and may attest that they do not have COVID symptoms—but

a facility cannot record this information alongside their name. In the event that contact tracing is needed due to a confirmed COVID case, a library department manager can check the schedule to determine which staff member was affected. In many cases, facilities have been able to accommodate this—allowing staff to step away when the kiosk automatically takes a photo, for example, or using "KCLS Staff" in lieu of individual names. When library and facility staff cannot come to an agreement about data privacy, the library will continue outdoor drop-off service instead of providing full service inside the building. Libraries and facilities failing to engage in dialogue around this new way of collecting information could result in a longer-term barrier to access for patrons should facilities adopt an approach that dictates that library staff who don't turn over their personal information to a kiosk simply cannot come to their buildings to provide service.

Automated collection of personal and biometric data by private companies could easily become the new normal in library outreach. The same types of kiosks currently proliferating in senior living communities might have broad appeal for all types of organizations, ranging from schools to offices or even to libraries themselves. COVID has changed the types of information organizations want to collect, such as visitor logs, body temperature, and health data. And it has changed how they collect that data, with wide-reaching, long-lasting ramifications for library staff data privacy.