

## Privacy Recommendations for Campus Reopening

The University needs to collect information from individuals to implement safety measures as we return to work and learn. Enhancing trust in the safeguards for personal data can increase participation needed for successful return-to-campus strategies.

Campus reopening programs may involve one or more of the following components:

- Symptom surveys/screening
- Temperature checks
- Job site/building access controls/building visitor logs
- Diagnostic testing
- Antibody testing
- Doctor notes
- Isolation housing
- Contact tracing (analog or digital)
- Case investigations
- Proximity tracking
- Research and modeling

As part of each of these components, personal data elements are collected, processed, or disclosed. While most privacy laws allow for public health activities, they require safeguards to be put in place, including focus on transparency and consent, limiting data collection for public health purposes, data minimization, security, and limits on retention, third-party sharing, and derivative uses of data.<sup>1</sup> Initiatives such as contact tracing generally involve collection of health data that if breached could trigger a requirement for formal notification under state law.

### The University should let individuals know

- About each program and about the data handling practices of each component
- How we seek their explicit consent for some program elements (e.g., app-based contact tracing)
- About a point of contact for questions and concerns

### Programs can address privacy by

- Limiting uses of information for public health activities
- Having a written protocol developed describing practices and procedures
- Sharing a communications plan developed for rollout
- Reviewing moves between stages along the resilience roadmap, adjusted to fit the circumstances
- Planning for an end date when data collection is no longer needed
- Providing oversight to accountability and to ascertain that measures are necessary and proportionate to their impact and effectiveness, and that use of personal data are firewalled from other functions<sup>2</sup>

### Data handling safeguards can include

- Collecting only if necessary and relevant for the stated purpose(s) and for the relevant population (e.g., teleworking employees generally would not need testing); and should distinguish between collection by a healthcare provider and a location

---

<sup>1</sup> [OECD Guidelines on the Protection of Privacy](#); [Privacy questions for COVID-19 testing and health monitoring](#)

<sup>2</sup> [World Health Organization. Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing](#)

- Specifying purpose for how data is used
- Preventing unauthorized use or disclosure (including applications that collect data)
- Documenting procedures to ensure data subject access rights (e.g., by students, represented staff, and the community)
- Limiting access to those with a need to know, and should distinguish between medical professionals providing healthcare and administrators protecting public health and facilitating University operations
- Retaining no longer than necessary, and maximally for the duration of a program
- Consulting with campus privacy officer for alignment with existing campus practices

The University is committed to preventing discrimination, intimidation, conflict, and bias, which could occur through certain uses of data. Accordingly, the University is carefully analyzing all initiatives for equity, diversity, and inclusion.