

EXPOSURE NOTIFICATION TECHNOLOGIES AND PRIVACY

House Innovation, Technology & Economic Development Committee
September 30, 2020

Presenters

Dr. Kathy Lofy

WA State Health Officer

Katy Ruckle

WA State Privacy Officer

Contact tracing background

- Case investigations and contact tracing have been in use for decades to slow the spread of infectious diseases (HIV, tuberculosis, hepatitis, etc.)
- Key public health tool that helps identify and stop chains of transmission, understand who is at risk, and inform public health response activities
- Local health leads this work; DOH supports
- COVID-19 case and contact definitions:
  - **A case:** A person with laboratory-confirmed COVID-19
  - **A contact:** Someone who has been within 6 feet of an infected person for at least 15 minutes



Contact tracing starts with a person who tested positive for COVID-19. This person will be advised to **stay home except to get medical care** until they are no longer contagious.



A trained interviewer will reach out to the person who has tested positive and ask for the contact information of close contacts. They will **not** ask for a social security number or about immigration status. Participation is voluntary.

A **close contact** is a person who has been within 6 feet, for 15 minutes or more, of someone who tested positive for COVID-19.

Next, the interviewer will reach out to the contacts to let them know they have been exposed.

Contacts stay home to watch for symptoms for 14 days after they were exposed.





If a contact tests positive, the process starts over again as a confirmed case.



They continue working with a public health professional to identify their contacts.



If there were no contacts, the process stops.

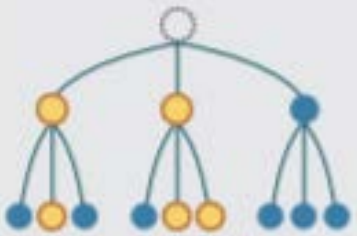


If a contact shows no symptoms for 14 days, they can return to normal activities.





If an infected contact is missed, the virus may spread to new contacts.



Use case: exposure notification technology





Exposure notification technology

- Apple and Google developed an underlying application program interface (API) and Bluetooth functionality
- API is incorporated into apps designed by public health worldwide; a solution is available without an app
- Apps can use Bluetooth proximity information to send notifications about exposure and recommend next steps
- Centralized vs. decentralized approach:
  - Google/Apple API requires decentralization – data is stored on user device Several EU countries started with centralized server, now switching to decentralized model
  - Decentralized is more privacy focused but less utility in the data for public health purposes
  - No geolocation data can be used by apps based on Google/Apple API

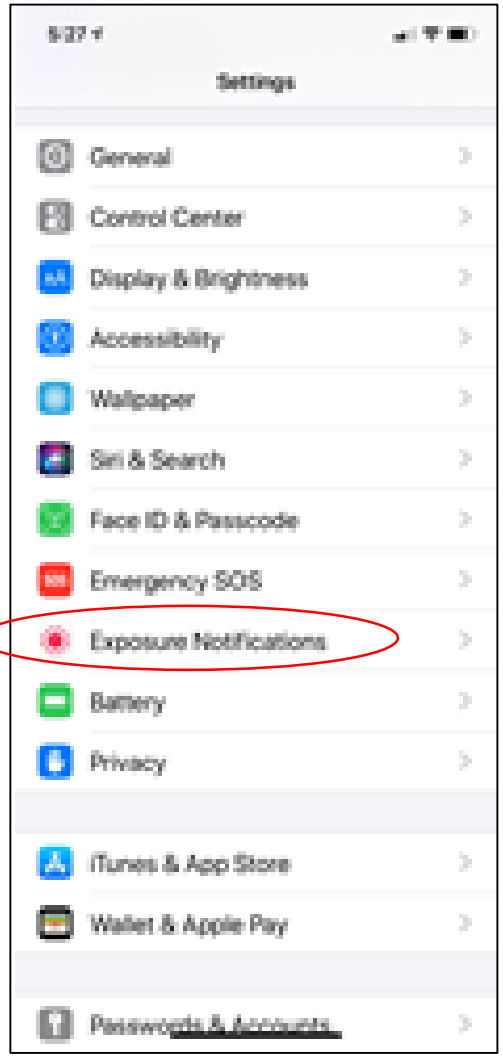
Apple/Google technology

- Bluetooth signals through Google/Apple API detect users in proximity (currently within 6 feet for 15 minutes or more).
- Their phones exchange anonymous key codes.
- If a user tests positive, they are instructed to enter a PIN to upload keys.
- Regularly phones look for matching keys and then alerts user of their potential exposure to someone who tested positive.
- User is directed to follow up with appropriate public health response (TBD).



Apple/Google exposure notification technology

- Technology exist on Apple and Google phones
- Use is voluntary
- Available in multiple languages
- Does not track location of user; only their proximity to others
- Users are anonymous
- COVID-19-positive users send PIN number to national server voluntarily



Use of exposure notification technology in Washington

- UW proven application (Common Circle) tested on the UW Medical Center Labor and Delivery floor
- State Exposure Notification Advisory Committee
  - Established in August by UW School of Public Health
  - Broad stakeholder representation
  - Purpose:
    - Review technologies
    - Make recommendations to DOH on implementation of technologies
- Next step: pilot project using an Apple/Google simplified adoption strategy (Exposure Notification Express)
  - Evaluate public health impacts
- Site of pilot not yet selected

Privacy principles for Washington State Agencies

- Lawful, fair, and responsible use
- Security
- Individual participation
- Data minimization
- Purpose limitation
- Transparency and accountability
- Due diligence

Privacy considerations in public health surveillance

- Privacy and confidentiality are cornerstones of public health data collection. Without trust that health information will be protected, public health suffers.
- RCWs and WACs lay the foundation for confidentiality practices when handling sensitive health data.
- HIPAA does not apply to protected health information (PHI) provided to DOH, but the Health Care Information Act (RCW 70.02) and other laws do.
- Identifiable patient data is exempt from disclosure (under RCW 43.70.050(2), RCW 70.02, and provisions of WAC 246-101 (notifiable conditions rules)
- OCIO Policy 141.10 – Securing Information Technology Assets

Data that contact tracers or case investigators **DO NOT** ask for

- Social Security Number (full or last four digits)
- Driver's license number or WA ID #
- Student, military, or passport ID number
- Health insurance policy number or health insurance ID number;
- Biometric data;
- User name or email address in combination with a password or security answers that permits account access
- *Any* financial information including:
  - account numbers,
  - credit or debit card numbers, or
  - any required security code, access code, or password that would permit access to an individual's financial account
- Marital status
- Immigration status



Washington State Department of Health is committed to providing customers with forms and publications in appropriate alternate formats. Requests can be made by calling 800-525-0127 or by email at civil.rights@doh.wa.gov. TTY users dial 711.