

<<Return Address>>  
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>  
<<Address1>> <<Address2>>  
<<City>>, <<State>> <<Zip>>

<<Date>>

### Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

This letter is to inform you that your personal information was inadvertently disclosed. This letter also provides additional information about the disclosure and what you can do to protect your personal information.

#### What Happened

You were enrolled in the University of Washington (UW) Husky Coronavirus Testing (HCT) research study being conducted by Dr. Helen Chu in the UW Department of Allergy and Infectious Diseases. This research study involved collecting nasal swab samples for detecting COVID-19 illness and collecting personal information from you.

On February 4, 2022, a research data file that contained your personal information was inadvertently uploaded by the research team to a public website. Within minutes, the research team became aware of the event and removed the data file from the website. The website administrators were also instructed to delete the data file from their system. This was completed the same day the data file was inadvertently uploaded on February 4, 2022.

On February 16, 2022, this event was reported to the UW Human Subjects Division and the UW Privacy Office. Through our joint investigation we learned that the data file was available on a publicly viewable website for approximately 30 minutes. The system logs indicate that a limited number of external users viewed the research study repository that contained the data file, but the system logs do not contain detailed information about the individual users or how they interacted with the data file. Thus, the UW is unable to determine if your personal information was or was not accessed by an unauthorized individual. On March 8, 2022, the Privacy Office determined that the UW would inform you about the inadvertent disclosure of your personal information and coordinated the UW's next steps with the Institutional Review Board for the research study. On March 24, 2022, the Institutional Review Board for the research study also determined that you should be notified of the inadvertent disclosure.

#### What Information Was Involved

The data file contained the following personal information which may apply to you and your participation in the research study:

- First and last name
- Date of birth
- Address
- Phone number
- Symptom duration
- COVID-19 test result/from sample tested on January 10th, 2022
- Other demographic information
- Other research study information

#### What We Are Doing

The research team has implemented additional data checks, updated workflows and processes, and developed procedures to de-identify personal data during certain phases of their work to help protect personal data.

### **What You Can Do**

Again, at this time, there is no evidence that your information has been misused. However, IDX representatives have been fully versed on the incident and we encourage you to contact IDX with any questions or concerns you may have by calling [\[telephone number\]](#) or going to [\[url\]](#). IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

### **For More Information**

Please call [\[telephone number\]](#) or go to [\[url\]](#) for assistance or for any additional questions you may have. The UW is committed to protecting the privacy of its research subjects. We are sorry for any concern this may cause you.

Sincerely,

ANN W. NAGEL  
University Privacy Officer  
Associate Vice Provost / Privacy  
UW Privacy Office / Academic and Student Affairs  
[privacy.uw.edu](http://privacy.uw.edu)

(Enclosure)



## Recommended Steps to help Protect your Information

**1. Website.** Go to [url].

**2. Telephone.** Contact IDX at [telephone number] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**3. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**4. Place Fraud Alerts** with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**5. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**6. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.