

DATA USE AGREEMENT

This Data Use Agreement ("Agreement") is made and entered into as of this 15 day of October, 2021 ("Effective Date"), by and between Secretaria de Salud, dependencia de Administración Pública centralizada del Gobierno del Estado de Coahuila de Zaragoza, a public health authority ("PHA"), with an address at Victoria #312, Zona Centro, CP. 25000, Saltillo, Coahuila, México and The MITRE Corporation ("MITRE"), a not-for-profit corporation with an address at 7515 Colshire Drive, McLean, VA 22102, United States of America.

WHEREAS, the PHA has elected to utilize the Exposure Notification Express technology ("ENX"), developed by Apple and Google; and

WHEREAS, the PHA acknowledges and agrees that the non-personally identifiable exposure notification data ("Data") gathered from individual mobile device users who have affirmatively consented via an opt-in option to enroll in ENX is being cryptographically bifurcated to protect privacy; and

WHEREAS, the PHA has designated Google and the Internet Security Research Group ("ISRG") to receive the privacy protected Data, using private keys issued to the PHA, and the Data is seamlessly sent via a privacy-respecting system for the collection of aggregate statistics ("Prio") to Google and ISRG; and

WHEREAS, the PHA acknowledges that the privacy protected and secure Data is then sent by ISRG and Google to MITRE, as the trusted third party, to combine the Data elements and conduct analytics on the Data ("Analytics"); and

WHEREAS, the Analytics will assist the PHA in tracking the trajectory of COVID-19 and monitor the effectiveness of the ENX, and the Analytics will be presented to the PHA via visualizations on a secure and privacy preserving portal, the Exposure Notification Privacy Analytics System ("ENPA Portal"), that is managed by MITRE and further described in Attachment A.

NOW, THEREFORE, PHA and MITRE hereby agree to the following terms and conditions in this Agreement:

1. PHA Obligations

- a. The PHA acknowledges and accepts their separate agreement to the ENX Google Analytics Servers Requirements ("Google Terms") described in Exhibit 1, attached hereto and incorporated herein by reference.
- b. The PHA acknowledges and accepts their separate agreement to the ENX Apple Analytics Servers Requirements ("Apple Terms") described in Exhibit 2, attached hereto and incorporated herein by reference.
- c. The PHA acknowledges and accepts their separate agreement to the ISRG Prio Subscriber Agreement and Amendment ("ISRG Terms") described in Exhibit 3, attached hereto and incorporated herein by reference.
- d. PHA acknowledges and agrees that Apple, Google, and ISRG are third party beneficiaries of this Agreement (collectively referred to as "Beneficiary") and that they have the full right to enforce the terms and conditions stated within their specific exhibit as if they were a signatory hereto.

2. MITRE Obligations

- a. MITRE shall share and disclose PHA specific Analytics, derived from the Google and ISRG deliverance of privacy protected PHA Data to MITRE, only with the PHA entity that originally provided the underlying Data, except as otherwise provided in Section 2d.
- b. Analytics will be shared via visualizations with that specific PHA via a secure password protected portal ("Portal") that is administered by MITRE.

- c. MITRE shall provide the PHA with the option to download their specific Data via an application programming interface ("API") from the ENPA Portal.
- d. The PHA has the sole discretion to authorize MITRE to share with other third parties, as vetted by MITRE, the PHA's Analytics via affirmatively selecting access right options on the ENPA Portal.
- e. MITRE shall protect the privacy and security of the Data and the resulting Analytics with commercially acceptable means, and no less rigorously than it protects its own sensitive information, but in no case less than reasonable care.
- f. MITRE will implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the security, integrity, and availability of the Data and the resulting Analytics.
- g. MITRE shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities while MITRE has responsibility for the Data and the resulting Analytics under the terms of this Agreement.
- h. MITRE shall report any confirmed Data breach to PHA promptly upon discovery, both orally and in writing. MITRE's report will identify: (i) the nature of the unauthorized access, use or disclosure, (ii) the Data accessed, used or disclosed, (iii) the person(s) who accessed, used and disclosed and/or received Data (if known), (iv) what MITRE has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (v) what corrective action MITRE has taken or will take to prevent future unauthorized access, use or disclosure.

3. Representation and Warrant

- a. Each party represents and warrants this Agreement complies with the party's domestic laws relating to the use and disclosure of electronic data as set forth herein and each party will advise the other of any material changes in domestic laws that would substantially frustrate, impair, or prevent any party's performance under this Agreement.

4. Term, Termination, and Disposition of Data

- a. *Term.* This Agreement shall be effective as of the Effective Date and shall continue until the Agreement is terminated by the parties in accordance with the provisions of Section 4.b.
- b. *Termination.* PHA and/or MITRE may terminate this Agreement:
 - i. immediately if either party determines that the other party has breached or violated a material term of this Agreement; or
 - ii. upon three (3) days notice if it is in the best interest of either party, as deemed by that party in its reasonable sole discretion to do so; or
 - iii. automatically upon the parties signing a new Agreement; or
 - iv. automatically after a period of two (2) years from the Effective Date.
- c. *Notice.* Notice of termination shall be sent in writing to the respective signatory of this Agreement at the address list above.
- d. *Disposition of Data.* Upon termination of this Agreement, MITRE agrees to destroy all specific PHA Data in MITRE's possession upon receipt of a written instruction by PHA to MITRE, excepting PHA Data that is already embedded in any authorized combined Analytics with other PHAs' Data.

5. EXCLUSION OF DAMAGES

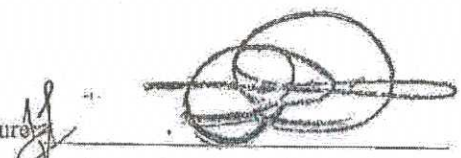
IN NO EVENT WILL EITHER PHA/MITRE BE LIABLE TO THE OTHER OR TO ANY THIRD PARTY FOR ANY INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES ARISING OUT OF, OR IN CONNECTION WITH THIS AGREEMENT, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), AND WHETHER OR NOT A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

6. Miscellaneous Terms.

- a. *Amendment.* PHA and MITRE agree that amendment of this Agreement may be required to ensure that PHA and MITRE comply with changes in domestic laws and regulations relating to the privacy, security, and confidentiality of the Data and/or Analytics.
- b. *Order of Precedence.* To the extent that any provision within Sections 1 through 6 of this Agreement conflicts with the provisions of any other agreement or understanding between the parties with respect to use of the Data and Analytics provided hereunder, this Agreement shall control. However, notwithstanding, the terms and conditions within the Exhibits shall take precedence and control as it relates to the PHA's agreement with a specific Beneficiary.
- c. *Counterparts.* This Agreement may be executed in one or more counterparts. Delivery of an executed counterpart of this Agreement by facsimile or a .pdf data file or other scanned executed counterpart by email shall be equally as effective as delivery of a manually executed counterpart of this Agreement. The parties to this document agree that a copy of the original signature (including an electronic copy) may be used for any and all purposes for which the original signature may have been used.
- d. *Use of Name.* Each party shall not use the name of the other party in any press release or other publicity document without the prior written approval of the other party.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the dates set forth below.

PHA


Signature: 

Printed Name: Dr. Roberto Berral Gómez

Title: Secretario de Salud

Date: 13 de octubre de 2021.

MITRE

Signature: 

Printed Name: DENA KOZANAS

Title: ASOC. GC + CPO

Date: 10-14-2021

Attachment A

Description of the Exposure Notification Private Analytics System

Exposure Notifications Private Analytics (ENPA) is a system built by MITRE, Apple, Google, Internet Security Research Group (ISRG), National Institutes of Health, and the Linux Foundation (collectively, the Parties) to provide detailed analytics to public health authorities (PHAs) utilizing Apple and Google's Exposure Notification Express (ENX) for COVID-19. The analytics will assist PHAs in tracking the trajectory of the disease and monitor the effectiveness of the exposure notification service. ENPA data will be derived from the ENX service. Aggregate analytic data will be presented to health officials through a cryptographically secure method to ensure user's privacy and anonymity. At no point will the Parties or PHAs know a user's specific analytic information, and users have the choice to "opt in" by downloading the application ("APP") or "out of" providing analytic information by deleting the APP.

As an independent, objective, and trusted third-party, MITRE will manage and maintain a portal for public health authorities to access ENPA data in their jurisdictions. This portal will feature easy-to-understand visualizations tracking data from Exposure Notification Express-enabled phones.

MITRE's visualizations and analytics show frequency of mobile phone alerts, how users interact with the alerts, and current trends. All analytic data is anonymized and aggregated. MITRE does not receive, process, or store any personally identifiable information and/or health information via ENPA.

Exhibit 1

ENX Google – Analytics Servers Requirements

“EN Analytics” (or “Exposure Notifications Analytics”) are the aggregated metrics relating to End Users’ use of the PHA Application that can be made available to the PHA.

“EN Analytics Servers” means the secure servers that PHA has designated to generate EN Analytics.

1. The owner/operator(s) (“Operators”) of EN Analytics Servers shall only process the data it receives or has access to in order to provide EN Analytics to PHA in accordance with a privacy-preserving system functionally equivalent to the code located at <https://github.com/abetterinternet/prio-server/> (as may be updated from time to time). The EN Analytics Servers may only disclose EN Analytics to the applicable PHA. The EN Analytics Servers may not disclose or reveal individual data contributions.
2. The Operators of the EN Analytics Servers may not (and may not attempt to) re-identify EN Analytics data.
3. The Operators of the EN Analytics Servers may only retain data related to EN Analytics for as long as necessary to provide EN Analytics to PHA (not to exceed one week after aggregation).
4. The Operators of the EN Analytics Servers shall deploy all applicable security updates and obtain a security audit from a trusted third-party.

Exhibit 2

ENX Apple – Analytics Servers Requirements

“EN Statistics” means the aggregated and anonymized statistics derived from PHA’s use of the Exposure Notifications technology.

“Analytics Servers” means the secure servers that PHA has designated to receive and process EN Analytics Data and EN Statistics.

“EN Analytics Data” means the (1) limited non-personally identifying analytics data that users may consent to share with PHA from their device and (2) the summed versions of such data that are used to create EN Statistics.

1. You shall access, receive, and process EN Analytics Data and EN Statistics in accordance with a privacy-preserving statistics aggregation system (“Prio”) that must be functionally equivalent to the code located at <https://github.com/abetterinternet/prio-server/>, and solely for the purpose of providing EN Statistics to PHA. Your Analytics Servers shall only disclose EN Statistics created in accordance with Prio to PHA. You shall only disclose EN Analytics Data that has been summed to the other designated Analytics Server. You shall not disclose EN Analytics Data that has not been summed under any circumstances.
2. You shall not attempt to re-identify the EN Analytics Data.
3. You shall only retain data used to create the EN Statistics, including the EN Analytics Data, for as long as required to create EN Statistics, which shall be approximately forty-eight (48) hours after aggregation, but in no case longer than one week after aggregation.
4. You shall deploy all applicable security updates to Your server software and obtain a security audit from a trusted third-party.

Exhibit 3

ISRG Prio Services Subscriber Agreement

This Subscriber Agreement (this "Agreement") is a legally binding contract between you and, if applicable, the company, organization or other entity on behalf of which you are acting (collectively, "You" or "Your") and Internet Security Research Group ("ISRG," "We," or "Our") regarding Your and Our rights and duties relating to Your use of Prio technology services offered by ISRG. If you are acting on behalf of a company, organization or other entity, you represent that you have the authority to bind such entity to this Agreement.

1. Definitions and Terms

"Aggregate User Data" — Data relating to Application Users that contains only aggregate information about such Application Users and no information that is specific to any single Application User.

"Application" — A software application operated or distributed by You that collects data relating to the end user thereof.

"Application User" — The end user of an Application.

"ISRG Prio Services" — The electronic services offered by ISRG, as described at: <https://abetterinternet.org/prio/>

"Private Key" — A key kept secret by its holder and which is used in public key cryptography to create digital signatures and to decrypt messages or files that were encrypted with the corresponding public key.

"Raw User Data" — Any data relating to one or more individual Application Users, which data is collected by an Application and is non-aggregate.

"User Data" — Raw User Data and Aggregate User Data, collectively.

2. Agreement Term

2.1 Effective Date of Agreement

This Agreement is effective on the first submission of Raw User Data by You, or on Your behalf, to ISRG Prio Services.

2.2 Term

This Agreement will remain in force during the entire period during which Raw User Data is being submitted by You, or on Your behalf, to ISRG Prio Services, through the time during which ISRG retains (has not yet deleted) Your User Data.

2.3 Survival

Sections in this Agreement concerning privacy, indemnification, disclaimer of warranties,

limitations of liability, governing law, choice of forum, and limitations on claims against ISRG, shall survive any termination or expiration of this Agreement.

3. Your Warranties and Responsibilities

3.1 Warranties

By using ISRG Prio Services:

- **You warrant** to ISRG and the public-at-large that You will only provide ISRG with a portion of each Application User's Raw User Data such that ISRG will never be able to construct a complete and de-anonymized copy of any particular Application User's data.
- **You warrant** to ISRG and to the public-at-large that you will not request access to, or undertake any effort to obtain, any Raw User Data from ISRG, including that which was submitted to ISRG by You or on Your behalf.
- **You warrant** to ISRG and the public-at-large that You will not undertake any other actions which might compromise the integrity of the Prio systems intended to protect the privacy of Application Users.
- **You warrant** to ISRG and the public-at-large that You have taken, and You agree that at all times that You will take, all appropriate, reasonable, and necessary steps to maintain control of, secure, properly protect and keep secret and confidential any Private Keys that are involved in the protection of User Data.

3.2 Rights in User Data

ISRG will not acquire any ownership rights in any User Data. You may request that ISRG delete User Data at any time.

3.3 Indemnification

You agree to indemnify and hold harmless ISRG and its directors, officers, employees, agents, and affiliates from any and all liabilities, claims, demands, damages, losses, costs, and expenses, including attorneys' fees, arising out of or related to: (i) any misrepresentation or omission of material fact by You to ISRG, irrespective of whether such misrepresentation or omission was intentional, (ii) Your violation of this Agreement, (iii) any compromise or unauthorized use of User Data or associated Private Keys, or (iv) Your misuse of User Data. If applicable law prohibits a party from providing indemnification for another party's negligence or acts, such restriction, or any other restriction required by law for this indemnification provision to be enforceable, shall be deemed to be part of this indemnification provision.

4. ISRG's Rights and Responsibilities

4.1 Privacy

ISRG's collection, storage, use and disclosure of User Data in connection with ISRG Prio Services are governed by the ISRG Prio Services Privacy Policy at:

<https://abetterinternet.org/prio/>

4.2 Data Deletion

ISRG will delete Raw User Data provided to ISRG by You or on Your behalf within a reasonable time after ISRG has completed or otherwise terminated the processing thereof.

4.3 Disclaimer of Warranties and Limitation of Liability

ISRG Prio Services are provided "as-is" and ISRG disclaims any and all warranties of any type, whether express or implied, including and without limitation any implied warranty of title, non-infringement, merchantability, or fitness for a particular purpose, in connection with ISRG Prio Services.

Because ISRG Prio Services are sometimes offered free-of-charge or at below ISRG's cost, ISRG cannot accept any liability for any loss, harm, claim, or attorney's fees in connection with such services. Accordingly, You agree that ISRG will not be liable for any damages, attorney's fees, or recovery, regardless of whether such damages are direct, consequential, indirect, incidental, special, exemplary, punitive, or compensatory, even if ISRG has been advised of the possibility of such damages. This limitation on liability applies irrespective of the theory of liability, i.e., whether the theory of liability is based upon contract, warranty, indemnification, contribution, tort, equity, statute or regulation, common law, or any other source of law, standard of care, category of claim, notion of fault or responsibility, or theory of recovery. The parties agree that this disclaimer is intended to be construed to the fullest extent allowed by applicable law.

Notwithstanding the foregoing paragraph, if You have entered (or are entering) into a separate agreement with ISRG under which You agree to pay ISRG fees for ISRG Prio Services, and such agreement contains a provision that limits ISRG's liability in connection with ISRG Prio Services, then to the extent ISRG accepts more liability in connection with ISRG Prio Services under such provision than under the foregoing paragraph, such provision will govern and control.

By way of further explanation regarding the scope of the disclaimer, and without waiving or limiting the foregoing in any way, ISRG does not make, and ISRG expressly disclaims, any warranty regarding its right to use any technology, invention, technical design, process, or business method used in providing ISRG Prio Services. You affirmatively and expressly waive the right to hold ISRG responsible in any way, or seek indemnification against ISRG, for any infringement of intellectual property rights, including patent, trademark, trade secret, or copyright.

5. Additional Terms

5.1 Governing Law

The parties agree that the laws of the State of California govern this Agreement, irrespective of California's choice of law and conflicts of law principles.

5.2. Choice of Forum

Any claim, suit or proceeding arising out of this Agreement must be brought in a state or federal court located in San Jose, California.

5.3 Limitation on Claims against ISRG

Any claim, suit or proceeding against ISRG arising out of this Agreement must be commenced within one year of any alleged harm, loss, or wrongful act having occurred.

5.4 No Third-Party Beneficiary

This Agreement does not create rights in favor of any third parties. Furthermore, it is the express intent of the parties that this Agreement shall not be construed to confer any rights on any third party.

5.5 Entire Agreement

This Agreement, together with any documents incorporated by reference in any of the foregoing, constitutes the entire Agreement between You and ISRG concerning the subject matter hereof.

5.6 Amendment

ISRG may modify this Agreement from time to time. Each modified version of this Agreement will be posted to ISRG's Prio Services website (abetterinternet.org/prio/) at least fourteen (14) days before it becomes effective. If such new version contains material changes and You have provided ISRG with an email address, ISRG will send an email to such address notifying You of such new version at least fourteen (14) days before it becomes effective.

5.7 Severability

If any provision of this Agreement is found to be invalid, unenforceable, or contrary to law, then the Agreement will be deemed amended by modifying such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this Agreement.

5.8 Authorization of ISRG to Send Emails

By entering into this Agreement, You authorize ISRG to send You emails relating to Your use of ISRG Prio Services.

ISRG may send You such emails using any email address You provide to ISRG or an address that is publicly associated with You.

Version 1.0
November 13, 2020