TEMPLATE

Utility Data Access Plan

SUBMITTED TO:

U.S. Department of Energy

Office of State and Community Energy Programs

To request a Microsoft Word version of this template, please visit:
www.missiondata.io/ira

MISSION DATA

TABLE OF CONTENTS

GLOSSARY

Advanced M&V Software Provider	A software vendor that provides measurement and verification ("M&V") services pursuant to the IRA's requirement that the Secretary of Energy establish an open-source, advanced measurement and verification software for determining and documenting the monthly and hourly (if available) weather-normalized energy use of a home before and after the implementation of a home energy efficiency retrofit.
Data Manager	The Data Manager assists in gathering permission-based energy-related data from electric utilities, natural gas utilities, delivered fuel providers, and sensors (such as electric submeters)
GBC	Green Button Connect My Data, an automated, system-to-system method for transmitting energy usage, bills and account information to a third party with customer consent. GBC should not be confused with "Download My Data," which is not automated.
IRA	Inflation Reduction Act
Program Implementer	The entity contracted to [STATE] that provides efficiency and/or electrification programs

INTRODUCTION

Pursuant to the U.S. Department of Energy's ("DOE" or the "Department") *Utility Data Access Guidelines* and the Inflation Reduction Act's ("IRA") Section 50121 requirements for Home Energy Performance-Based, Whole-House Rebates ("HOMES"), [STATE] is pleased to provide this *Utility Data Access Plan* for review and approval by the Department.

Having reviewed all of the DOE requirements, including the *Program Requirements & Application Instructions* (updated October 13, 2023), *Data Tools and Requirements Guide* (updated October 13, 2023), and the *Utility Data Access Guidelines* (dated July 27, 2023), [STATE] is confident in our plan to meet all program goals. Specifically, this *Utility Data Access Plan* addresses DOE's overall requirement of providing risk-based security controls by establishing (1) clear data definitions, (2) a detailed inventory of the entities that will receive customer data, and (3) appropriate safeguards and requirements for each entity and data type. [STATE] also provides assurance to DOE that [STATE] will adhere to the DOE and Pacific Northwest National Laboratory ("PNNL") workflow.

As DOE has recognized, each state may rely upon numerous sources for customer energy consumption data, ranging from electric and gas utilities to delivered fuel providers to customer-installed sensors, all of which are essential to establishing whole-home energy usage. Heterogeneity of data access methods and practices is inevitable, and [STATE] is no exception. Recognizing this complexity, [STATE] has established detailed plans from core data privacy and security principles, as explained in the pages below. When coupled with a *Privacy and Risk Assessment* – required by DOE within 60 days prior to planned rebate program launch – [STATE] will have comprehensively addressed the Department's requirements.[1] [STATE] will submit, in a separate document, our independently-reviewed *Privacy and Risk Assessment* in due course.

If the Department has any questions, please contact the program leads below.

Sincerely,

____

[STATE: Add Appendix justifying any deviations from DOE/PNNL workflows, if applicable. For more information: https://www.pnnl.gov/projects/rebate-tools]

[1] Requirement 3.1.6.1 of Program Requirements & Application Instructions, page 21.

OVERVIEW

[STATE] has identified that it will need to rely upon numerous data sources for customer energy consumption data in order to serve all communities within [STATE]. The sources range from electric and gas utilities to delivered fuel providers to customer-installed sensors. For any given site, the data source may be singular or come from multiple sources to establish the whole-home energy usage before and after an intervention. Other customer metadata (i.e., location, income eligibility, etc.) is not within the scope of this *Utility Data Access Plan*.

The flows of energy usage data identified for [STATE] (electric, gas, propane/fuel oil, etc.) are shown in Figure 1 below:

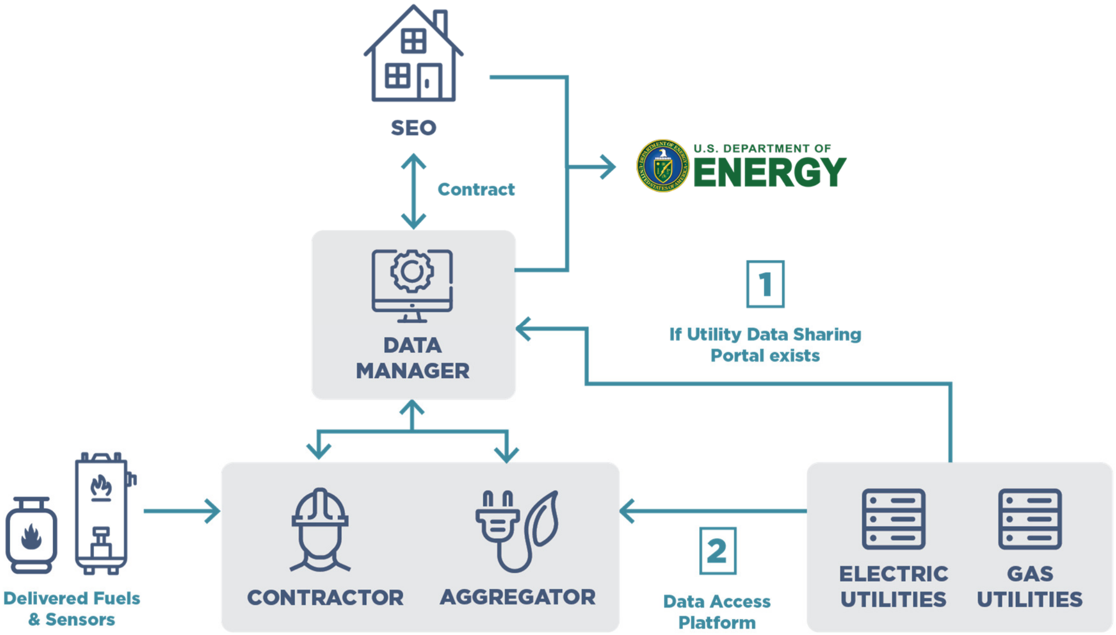


Figure 1. *Flows of energy usage data*

[SPECIFY WHETHER THE DATA MANAGER IS A VENDOR TO STATE, OR IS CONTRACTED BY THE PROGRAM IMPLEMENTER OR ANOTHER ENTITY.] The Data Manager assists in gathering permission-based energy-related data from electric utilities, natural gas utilities, delivered fuel providers, and sensors (such as electric submeters).

[STATE: Alternate showing ENERGY STAR Portfolio Manager, if applicable]

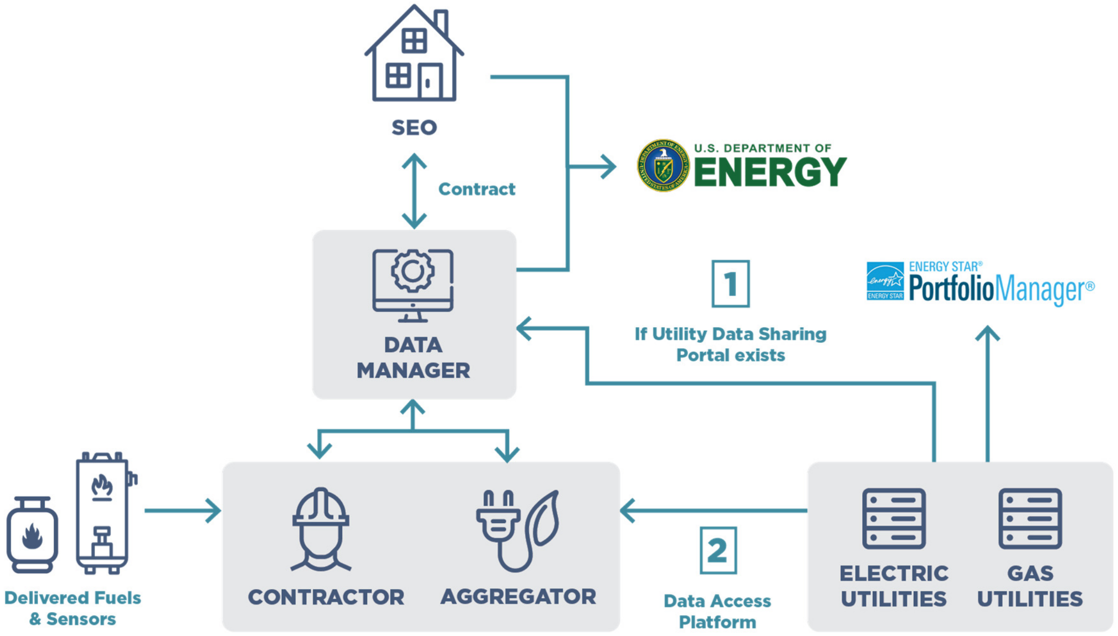

SEO
Contract
U.S. DEPARTMENT OF ENERGY
DATA MANAGER
1
If Utility Data Sharing Portal exists
ENERGY STAR® Portfolio Manager®
Delivered Fuels & Sensors
CONTRACTOR
AGGREGATOR
2
Data Access Platform
ELECTRIC UTILITIES
GAS UTILITIES

Figure X. *Data Manager and ENERGY STAR Portfolio Manager*

GUIDING PRINCIPLES

In developing this Data Access Plan, [STATE] has been driven by the following guiding principles:

- **Data Management Tools Must Be Market-Ready Solutions.** In order to ensure that residents receive Congressionally-appropriated funds for HOMES retrofits as soon as possible, we chose several technology solutions that have market-ready solutions that can be implemented quickly. While experimentation with new software technologies has its rewards, we opted for those that have been validated with a broad user base. This helps reduce technical and implementation risk and improves cybersecurity preparedness.
- **Tools for Contractors Must Be Easy to Use and Well-Suited to the Program.** Contractors should be able to use tools most suitable to their participation in the program. Requiring our state's contractors to implement untested tools or hard-to-use processes creates challenges in terms of education, training, support and delays in program administration. We chose to use [DATA MANAGER] because many contractors already use them, ensuring a more efficient use of federal funds.
- **Use Green Button Where Possible and Practical.** In our state, Green Button Connect My Data (GBC) has been implemented by [LIST UTILITIES] and we intend to use those data sharing portals as much as possible. However, there are limitations on our current use of GBC:

    - [IF APPLICABLE] Vendors have indicated that [UTILITY's] GBC suffers from quality issues that prevent us from relying on it. We will continue to work with [UTILITY] to implement improvements.
    - The following energy usage data sources do not yet support GBC: [LIST UTILITIES OR DELIVERED FUEL PROVIDERS].

We recognize that it will take time to make universal GBC availability a reality. Thus, we are leveraging GBC where possible, while continuing to pursue consistent and high quality GBC implementation by all of our state's electric and gas utilities.

- **Tools Must Provide Equitable Coverage Across [STATE].** It is important to ensure that the tools chosen can serve all communities, not just those served by large investor-owned utilities. We seek to support information-gathering from rural, consumer-owned, or smaller utilities, which are often farther behind in their ability to provide secure, automated energy data accessibility.
- **Promote Market Transformation.** Rather than asking our utilities to provide "one-off" solutions for accessing energy usage data that would not outlive HOMES or would not be available for residents to use outside of the context of HOMES, we selected established Data Managers (defined below) and support Green Button implementation so that federal investments become catalysts for ongoing market transformation, even after HOMES funding has ended.
- **Consistent with DOE/PNNL Workflows**: Although Figure 1 is not formatted as a workflow, [STATE]'s Utility Data Access Plan is entirely consistent with the DOE/PNNL Workflows.[2] Vendors will handle automated interactions involving energy usage data as well as customer income verification, a topic which is not addressed in this *Utility Data Access Plan*.

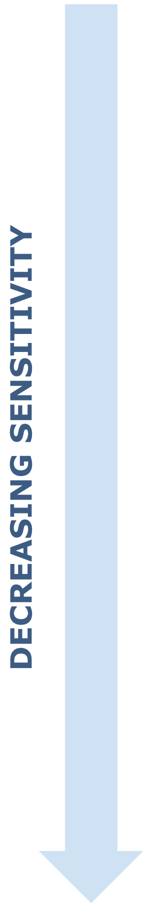
SAFETY AND SECURITY OF ENERGY CONSUMPTION DATA

DATA DEFINITIONS

The first step to ensuring the safety and security of energy usage data is clearly defining what data is being used in the administration of HOMES funds. For example, household-specific and personally-identifiable information (PII) data carry very different risks of privacy intrusion than, say, total

[2] https://www.pnnl.gov/projects/rebate-tools

kilowatt-hours (kWhs) of electricity saved across 1,000 homes. Moreover, the mitigation approaches for each data type depends upon the data and processes in question. Thus, prior to understanding the risks of each data type, we have established the following definitions and use them as capitalized terms throughout the *Utility Data Access Plan*:



1. **Customer Credentials**: The customer's username and password to their electric or gas utility's web portal. It is not possible to administer HOMES without some level of customer credential-sharing, because not all energy data providers (i.e., utility, delivered fuel provider, etc.) are going to provide an automated integration. Customer credentials receive the highest level of security.

2. **Personally-Identifiable Information:** Any information that is tied to a person or household including, but not limited to, names, addresses, telephone numbers, etc.

3. **Energy Data**: Individual household usage of electricity (kWh), natural gas (therms or cubic feet), propane (gallons), fuel oil (gallons), etc. Includes bill details and amounts (dollars). Unless copies of bills are specifically referenced, Energy Data excludes address, names or other personally-identifiable information. Zip code is included for weather normalization purposes.

4. **Whole-Building Usage Data**: The energy usage from multiple metered fuels (electricity, natural gas, etc.) in a single value so that the whole building's energy usage is captured for a specific time period (hourly, daily, monthly or annually).

5. **Portfolio Data**: Calculated *changes* in energy consumption (not individual household energy consumption or Whole-Building Usage Data), with or without other metadata such as location, home vintage, eligibility information, etc. Portfolio Data is always an aggregation of homes' changes in energy consumption.

CLARIFYING THE DISTINCTION BETWEEN SECURITY REQUIREMENTS ESTABLISHED BY UTILITIES VERSUS REQUIREMENTS ESTABLISHED BY HOMES

In [STATE], the following organizations are involved in both administering HOMES and are contracted with electric and/or gas utilities to provide demand-side management or other services:

- [LIST]

[IF THIS IS A NULL SET, THEN STATE SHOULD DELETE THIS SECTION ALTOGETHER BECAUSE IT IS NO LONGER RELEVANT.]

It is necessary to clarify that these entities' activities done on behalf of utilities are out of scope of this *Utility Data Access Plan*. By virtue of being a vendor to utilities, these entities are already subject to utilities' rigorous data security and privacy requirements and do not need to be addressed here. However, the entities' activities done on behalf of [STATE] (or on behalf of contractors, aggregators, etc.) for administering HOMES ***are*** within scope of this *Utility Data Access Plan*.

This *Utility Data Access Plan* will not speak to utilities' cybersecurity policies or practices in any way. If DOE has questions about utilities' privacy or security measures, [STATE] encourages DOE to pose such questions to the utilities directly.

DATA RECIPIENT INVENTORY

The second step to ensuring data safety and security is an inventory of the entities who take custody of energy usage data.

1. **Data Manager**: Vendors for information technology. Vendors serve in the capacity of helping [STATE], Program Implementers, Contractors or Aggregators access customer utility data with customer permission. Data Managers could store Customer Credentials, but Customer Credentials will not be shared with, or accessible to, any other party, including [STATE].
2. **Program Implementer:** [NAME], contracted to [STATE], that provides efficiency and/or electrification programs.
3. **Advanced M&V Software Provider:** A software vendor that provides measurement and verification ("M&V") services pursuant to the IRA's requirement that the Secretary of Energy establish an open-source, advanced measurement and verification software for determining and documenting the monthly and hourly (if available) weather-normalized energy use of a home before and after the implementation of a home energy efficiency retrofit.
4. **Contractor**: The entity hired to perform assessments and install upgrades (i.e. installs heat pumps, insulation, etc.).
5. **Aggregator**: An entity that engages with multiple single-family homes and/or multifamily buildings for the purpose of combining or streamlining projects as allowed by the State.
6. **Utility**: A provider of electric, natural gas or steam services.

DATA RECIPIENT	DATA TYPE(S) HELD	TREATMENT
Data Manager	✓ Customer Credentials ✓ Energy Data ✓ Whole-Building Usage Data ✓ Portfolio Data	Privacy and security ensured through standard contracts or custom-negotiated contracts with vendors. DataGuard[3] is included in contract as well as SOC2 Type II compliance. [STATE insert specific security requirements here if the STATE contracts directly with Data Manager(s)]
Program Implementer	✓ Energy Data ✓ Whole-Building Usage Data ✓ Portfolio Data	
Advanced M&V Software Provider	✓ Energy Data ✓ Portfolio Data	[IF the Advanced M&V Software Provider is contracted to a utility, then enter "Defer to utilities' privacy and cybersecurity requirements."] [IF contracted to [STATE], then enter "Privacy and security ensured through contractual terms, including DataGuard and SOC2 Type II compliance. Energy Data is held strictly private, while Portfolio Data will be shared with market participants and potentially released publicly."]
Contractors	✓ Energy Data ✓ Whole-Building Usage Data ✓ Portfolio Data	Energy Data is provided via customer consent (i.e., opt-in). Contractor use of data is limited to the customer-authorized scope (e.g., "for an energy audit" or "for providing a retrofit and ensuring payment of rebates"). - Contractor will not be subject to SOC2/DataGuard. Data will be secured by the Data Manager according to the treatment above once it is received by the Data Manager. It would be impractical and/or impossible to hold contractors to identical data security requirements as to Data Managers. - Customer/homeowner holds Contractor harmless for claims how the Usage Data was accessed

[3] U.S. Department of Energy DataGuard Privacy Standard. https://www.smartgrid.gov/archive/data_guard

Aggregators	✓ Energy Data ✓ Whole-Building Usage Data ✓ Portfolio Data	Access to Energy Data is granted with customer consent (opt-in).
Utility	✓ Energy Data ✓ Whole-Building Usage Data ✓ Portfolio Data	Data categories listed are treated according to the utilities' policies and procedures for privacy and security.
State Energy Office	✓ Energy Data ✓ Whole-Building Usage Data ✓ Portfolio Data	[STATE to fill in]

GUIDING PRINCIPLES

[STATE] has taken the following guiding principles into account in program design and in selecting vendors and negotiating contracts.

- **Least privilege**: The authority of any vendor or entity within information technology systems should be limited to those that are necessary to do the job. Extra privileges – for example, the ability to modify Energy Data where merely read-only access is required – introduces unnecessary risks. Rather than relying solely on contractual provisions to restrain vendors' activities, enforcing technological limits on system access privileges is a best practice.
- **Data minimization**: A similar concept to "least privilege" is providing only the customer data that is necessary for the task at hand. For example, an aggregator should not have customers' banking information or social security numbers because that information is not necessary. In the case of Energy Data, vendors will be limited to gathering the same information that is available to the customer on the utility's website or on monthly utility bills. There may be information inadvertently captured on utility bills that is not needed by the HOMES program, such as whether a customer has past-due amounts; however, this information will not be shared with [STATE]. In the case of optimizing the program with advanced targeting analytics or establishing robust calculations of impacts, population data (i.e., usage data from non-participating customers in a specific region) may be necessary to complete the task.
- **Informed consent**: It is critical that customers are fully aware of the contents of the information they are being asked to share with contractors, aggregators, [STATE] and DOE. Thus, we have provided example screenshots of the authorization pages that customers will see. By designing these authorization pages with best practices in mind (such as simplicity and user-friendliness), we will ensure that customers are fully informed. In addition, given privacy concerns and 4th Amendment protections involving homes in particular, it is critical

for customers to understand that portions of their data will be shared with [STATE] and DOE, *even if some believe that the risk of re-identification is low*. If customers are not comfortable sharing their information with [STATE] or DOE for any reason, they can decline to receive rebates. Note: For the purposes of comparison group analysis as part of advanced M&V, it is unnecessary to secure informed consent because individual Energy Data is not shared beyond the Advanced M&V Software Provider, and contractual provisions prevent the Advanced M&V Software Provider from further disclosure.

- **Ensuring conformance with authorized scopes of use.** When a customer grants permission for a contractor to use his or her Energy Data for determining a HOMES rebate, it is critical that the contractor not exceed the scope of that authorized use. For example, having Energy Data shared with other service providers for unwanted marketing, or accessing energy usage beyond a customer-agreed timeframe, would exceed an authorized use. This principle is consistent with the U.S. Federal Trade Commission's 2012 guidance on consumer choice, which states that entities' use of customer data must be limited to "the context of the interaction"[4] and that any other uses of customer data require consent.

GREEN BUTTON SAFETY AND SECURITY

Many, but not all, exchanges of Energy Data will use GBC. GBC is a standard ratified by the North American Energy Standards Board and includes numerous technological features to ensure safety and security both during the authorization process and during transit. These features include:

- Mandatory Transport Layer Security v1.2 or later for encryption in transit
- Mandatory OAuth 2.0 (IETF RFC 6749), widely used for secure, user-specific, scope-limited authorizations
- Adherence to "Privacy By Design" – a concept recognized by many jurisdictions in which privacy is incorporated into all aspects of engineering design.

[COMPLETE THIS SECTION BELOW ONLY IF YOUR STATE PUBLIC UTILITY COMMISSION HAS ESTABLISHED GBC RULES ON DATA RECIPIENTS]

[4] U.S. Federal Trade Commission. 2012. *Protecting Consumer Privacy in an Era of Rapid Change* at p. 38. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

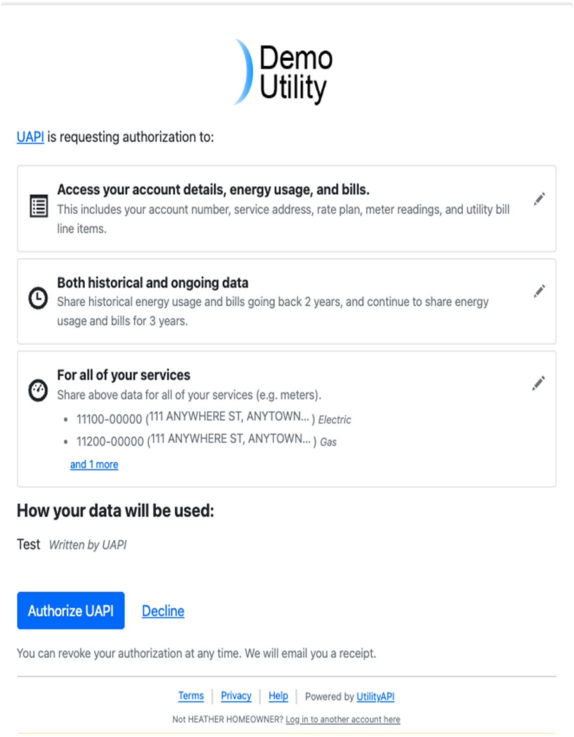
In addition to the technological measures incorporated into the GBC standard, [STATE PUBLIC UTILITY COMMISSION] has established the following additional eligibility criteria for any customer-authorized third party that receives energy usage, account or billing information from an investor-owned utility:

State	GBC Data Recipient Eligibility Criteria
California	Must provide contact info; agree to privacy terms; not be on the Commission-maintained list of "banned" third parties
Colorado	None. Electric Rule 3027(e) says, "Nothing in these rules shall limit a customer's right to provide his or her customer data to anyone."
Illinois	Must agree to abide by ICC-approved tariff, which includes privacy requirements
New York	Must sign a Data Security Agreement, which requires adherence to security requirements such as an information security policy, incident response procedures, role-based access controls, multi-factor authentication for administrative systems, a prohibition on storing customer data on unencrypted mobile devices, 24/7 anomaly monitoring, employee background screening and security awareness trainings
Texas	Must agree to Smart Meter Texas terms and conditions, which include limiting the use of customer data to the customer-authorized purpose and registering with a unique DUNS number
[STATE]	[LIST REQUIREMENTS]

INFORMED CONSENT

It is important that customers know what information will be shared, and with whom, prior to their consent. Examples below show how this will be displayed to the customer.

The consent to share Energy Data is a distinct part of program enrollment – it is not a footnote to a longer, contractual document between a customer and implementer. A separate consent form for Energy Data ensures the customer is fully aware of the circumstances surrounding their sharing.



Demo Utility

UAPI is requesting authorization to:

Access your account details, energy usage, and bills.
This includes your account number, service address, rate plan, meter readings, and utility bill line items.

Both historical and ongoing data
Share historical energy usage and bills going back 2 years, and continue to share energy usage and bills for 3 years.

For all of your services
Share above data for all of your services (e.g. meters).

- 11100-00000 (111 ANYWHERE ST, ANYTOWN...) *Electric*
- 11200-00000 (111 ANYWHERE ST, ANYTOWN...) *Gas*

and 1 more

How your data will be used:

Test *Written by UAPI*

You can revoke your authorization at any time. We will email you a receipt.

Not HEATHER HOMEOWNER? Log in to another account here

Figure X. *Example screenshot showing the consent form.*

METHODS FOR ACCESSING UTILITY ACCOUNTHOLDER DATA

Technology to access accountholder data will follow privacy, security, consent, authorization, and other requirements described above. Access to accountholder data can be provided in several ways depending on the capabilities of utilities and market actors. Data recipients will be able to utilize the best available technology that follows the above requirements to access accountholder data needed to serve their customers and the program.

As for accessing electricity and natural gas usage data, technology capabilities for Program Implementers, Contractors, Aggregators and Advanced M&V Software Providers generally fall into two categories:

1. Utility Data Sharing Portals

2. Data Access Platforms

Utility Data Sharing Portals: Utility data sharing portals are hosted information technology infrastructure built and maintained by the utility, or by a utility vendor, and are designed to provide registered third parties with authorized access to customer utility data. These portals require information technology investment from utilities, including up-front costs and ongoing operations and maintenance. Typical utility portals involve three core processes: (i) third party onboarding and management, (ii) customer authorization, and (iii) data gathering and transmission.

(i) **Third party onboarding and management:** Third parties register with the utility portal by providing some business information, the utility verifies each third party meets its eligibility criteria, and subsequently the third parties receive access keys to be used upon subsequent data requests.

(ii) **Customer authorization:** Customers authorize the utility to release their information to a specific registered third party. Customers enter their utility credentials or some other account-identifying information to the utility portal.

(iii) **Data gathering and transmission:** Only data published by the utility is gathered. Data types served by utility portals vary, and tend to be tied to specific use cases. The most universal is monthly or interval energy consumption. Portal types include: property management, building benchmarking, and historical consumption.

Green Button Connect (GBC) is an example of utility hosted data sharing portal, in which the utility or its vendor builds a dedicated channel specifically designed to serve data to registered third parties' customer authorized requests. Green Button Connect is a standards-based implementation that helps to reduce costs for all parties by providing a consistent protocol. (GBC should not be confused with Green Button Download My Data, which is not automated.) Some utilities have built non-GBC portals, such as ConEd in New York and the Smart Meter Texas platform.

Data Access Platforms: Data access platforms are provided by software companies who specialize in serving third party customer requests to access a specific utility account holder's data. Data access platforms are often unaffiliated with the utility, instead providing data access as a service to a wide variety of third parties, program administrators, and consumers. These companies arose in response to the natural mismatch between company footprints and utility service territories. For example, where large companies receive bills from tens or hundreds of utilities or serve customers across the country, they need uniform information to process and manage their energy consumption.

Data access platforms can be helpful to serve customers at the "long tail" of utilities, where smaller utilities (municipals, co-ops) may not have the means to stand up their own utility portals. Data access platforms can serve any number of third parties, including those that provide goods and services for the residential, commercial, and industrial sectors.

Similar to utility portals, data access platforms involve three core processes: (i) third party onboarding and management, (ii) customer authorization, and (iii) data transmission.

(i) **Third party onboarding and management:** Third parties (such as Contractors, [STATE] and Aggregators] register with the data access platforms as part of their customer onboarding process, establishing a business and technology relationship. Some eligibility criteria may be used by the platform to ensure that the third party meets their standards of use. As part of that relationship, the customer receives access keys to the data access platform.

(ii) **Customer authorization:** Customers authorize the data access platforms to act as their authorized agent and access their utility account in order to retrieve information. In most cases, customers provide their utility credentials (i.e., username and password) to the data access platform, which uses those credentials to fulfill its authorized service as the customer's agent.

(iii) **Data gathering and transmission:** In their role as customer-authorized agents, data access platforms use utilities' existing customer portals to access data. Therefore the only information they gather is that which is published by the utility to the customer (i.e., monthly bills, historical energy consumption, etc.).

PORTFOLIO-LEVEL MEASURED SAVINGS

[STATE] is implementing a measured version of HOMES. As such, data security is paramount. Data security is accomplished by requiring robust confidentiality measures in our contracts and requiring top notch security for Data Managers, Program Implementers and Aggregators. Our data-sharing practices ensure the integrity of data inputs within our system and the integrity of accurate and useful outputs.

The inputs crucial for energy savings calculations include individually-identifiable Energy Data. We will shield inputs through legally binding agreements such as Non-Disclosure Agreements (NDAs) and security accords. In addition, we will assess and evaluate the overall re-identifiability of individuals encompassed within a dataset. Our assessment is grounded in the synergy between contextual factors: the likelihood of an attack and the characteristics of the data which influence the probability of re-identification during an attack scenario. The assessment will drive the data transformations required to reduce identifiability so residual risks are appropriately managed. After calculations are complete, risk of re-identification are minimized for the derivative results and customer authorization as part of their agreement to participate in the program.

In [STATE's] measured program, the core output will be the derivative calculations of savings impacts made from individuals energy consumption data and summed for the portfolio. The portfolio-level measured impacts would be the final product for [STATE SEO] to review from the approved program implementer or open-source advanced M&V platform provider before reporting to DOE. Since the data is aggregated and derived from data for which customers directly authorized use, the output is not protected by an NDA or other secure agreements. If the individual results are required per PNNL data flow, then sharing may need to be protected by NDA. If customer authorization for all use cases (including DOE reporting and evaluation) is acquired at the time of the project there is no barrier to sharing and reporting disaggregated data.[5] The derivative data output is fully de-risked by anonymizing and aggregating it. Personally identifiable information (e.g. name, address, account number or meter identifier) will not be included in the energy savings derivative reporting data or any publicly available data.

[STATE] has developed this plan by leveraging examples from those who have had experience with these types of programs. Advanced M&V Software Providers have expertise in maintaining data pipelines and processing platforms in alignment with the strictest security expectations to inform their calculations. Their incoming data pipelines enable savings calculations for each project and site and then sum for portfolios of projects. An aggregated, portfolio view provides a consistent metric of program performance suitable for interim program reporting and is in compliance with DOE guidance for reaching the required savings threshold of 15% for a portfolio to be eligible for the rebates. Once a program cycle has been completed, the same results can be formatted for final reporting and, in many cases, used in lieu of an additional evaluation, especially if a comparison group has been tracked alongside the treatment group.

DATAGUARD PRIVACY STANDARD

The DataGuard Energy Data Privacy Program was developed in order to increase consumer confidence in the developing marketplace for data-driven energy services. Websites that feature the

[5] [STATE] acknowledges that DOE requires prohibitions against data selling and data sharing (page 21, *Home Energy Rebates Program Requirements & Application Instructions*). However, [STATE] believes this requirement is superseded by the informed consent of the customer. If the customer agrees to have their energy data shared with other entities or for research purposes, and the consent is validly obtained, then DOE's prohibition against "data sharing" in that instance is not applicable. After all, rigidly applying DOE's prohibition in 100% of cases would prevent [STATE] and DOE itself from receiving Energy Data.

DataGuard seal demonstrate that they adhere to a voluntary but rigorous set of privacy and security safeguards. Commitments to DataGuard are similar to privacy policies in the sense that they are representations of the organization's commitment to policies and practices in handling sensitive customer data. If the organization fails to adhere to its own stated policies in any way, affected customers may seek a remedy through state Attorneys General or the U.S. Federal Trade Commission, which has broad authority to penalize firms for unfair or deceptive trade practices.

[STATE] will contractually require the following participants to adhere to DataGuard throughout the term of the HOMES program:

- Data Managers
- Program Implementers
- Contractors
- Aggregators
- Advanced M&V Software Providers

STATE INFORMATION SECURITY REQUIREMENTS

[This space is reserved for state-specific information security requirements.]

CUSTOMER AUTHORIZATION, NOTIFICATION AND REVOCATION PROCESSES

DOE outlined four consent options that must be explicitly addressed in this Utility Data Access Plan: **opt-in**, **opt-out**, **open access** and **data aggregation.**

[STATE] will require customers to affirmatively **opt-in** to having their energy usage data shared with contractors, aggregators, [STATE] and DOE. Receiving a rebate is contingent upon the customer agreeing to share their energy usage data with certain entities (and subject to restrictions such as DataGuard) as described in this plan/

[STATE] will ***not*** use opt-out or open access consent methods. [STATE] believes these are inconsistent with state and federal best practices and could lead to negative outcomes such as privacy violations that could set back HOMES implementation. As a result of our decision to not use opt-out or open access methods, [STATE] will avoid spending time or resources establishing processes for monitoring and handling opt-out requests.

[FOR CALIFORNIA, NEW YORK OR OTHERS WITH ELECTRIC/GAS UTILITY COOPERATION RE: TARGETING AND DATA AGGREGATION] [STATE] intends to use data aggregation for the purpose of targeting customers. In this case, [UTILITY/STATE ENTITY] is able to analyze historical customer energy usage data and provide Program Implementers with the addresses of customers that are high energy users or would otherwise be a prime candidate for efficiency retrofits. The Program Implementer will ***not*** receive such customers' individual energy usage records unless and until consent has been granted.

Below we provide an overview below of the authorization, notification and revocation processes for each method of accessing energy usage data. Multifamily projects are treated separately because of the unique issues involving consent processes for whole-building energy usage data.

SINGLE FAMILY

For single family homes, the **primary purpose** will be clearly spelled out in (i) contractual documents for customers to sign and/or (ii) GBC authorization forms. Consistent with DataGuard, any use of customer data that goes beyond what the customer agreed to is not permitted. [STATE] will not permit any secondary purpose of Energy Data. Allegations of breaches or other unconsented uses of Energy Data will be investigated by [STATE] in collaboration with [STATE] Attorney General, with referrals made to the U.S. Federal Trade Commission where appropriate.

Below we outline the authorization, notification and revocation processes for each data access method:

Method	Authorization	Notification	Revocation
Delivered Fuels	Opt-in	None	The customer can cancel their enrollment with Program Implementer; decline to share future bills/invoices; or direct their fuel provider to stop sharing information with others.
Sensors[6]	Opt-in	Program Implementer will be responsible for	Program Implementer will be responsible for assisting customers with revocation requests.

[6] Includes electric submeters; smart electric panels; propane tank sensors; solar inverters; and electric vehicle chargers.

		providing annual notices to customers.	
Utility Data Sharing Portals	Opt-in	[STATE to fill in if applicable]	A customer can revoke at any time by calling the utility or by logging into the utility's web portal. In addition, [LIST UTILITIES] will automatically revoke an authorization if the customer moves out or closes his/her electric/gas account.
Data Access Platforms	Opt-in	Annual notices via email	Customers can revoke at any time. Customers also receive an email "receipt" at the time of authorization, and the receipt contains a link to manage authorizations.
Customer manually shares energy usage history (paper/email bills, Green Button Download My Data, etc.)	Opt-in	None	Disenrollment

[INSERT PRODUCT-SPECIFIC NOTIFICATION DETAILS, IF APPLICABLE]

Consistent with the principles of informed consent, [STATE] will require Program Implementers to explicitly mention in its contracts with customers that [STATE] and the U.S. Department of Energy will receive Energy Data. If the customer objects to this, they can decline to receive a rebate. Out of an abundance of caution, [STATE] believes this disclosure is reasonable and necessary even if energy usage data is not easily linked to a particular individual.

MULTIFAMILY

Whole-building aggregated usage data will be shared with ENERGY STAR on an opt-in basis.

Data access for multifamily buildings presents a special circumstance in implementing the HOMES and HEEHR programs for various reasons. First, multifamily buildings have various types of metering configurations that can make program participation, measurement, and verification challenging. The three (3) main types of multifamily metering configurations are:

1. **Whole Building Metering:** Whole building metering, also referred to as "master metering," represents a building where the entire building's energy usage is metered and billed by the serving utilities. Whole building metering doesn't separate common area and tenant area-specific energy and metered usage.
2. **Common Area Metering:** Common area metering represents a building where the building's common areas (i.e., lobby, garage, etc.) are metered and billed by the utilities separate from the tenants' energy usage.
3. **Tenant Area Metering:** Tenant area metering represents a building where the building's tenant areas are metered and billed by the serving utilities, separate from the common area metering. Tenant area metering can be done at a whole building level, meaning all units' energy usage is billed and metered at one "master meter," or tenant area metering can be done at an individual by individual tenant level.

Regardless of the metering configuration present at multifamily building seeking to participate in the HOMES and HEEHR, DOE's Program Guidance makes it clear that these properties provide the same level of data protection and security as single-family household.[7] As such, [STATE] will pursue a two-pronged strategy to ensure that eligible individual tenants and multifamily properties can participate in the HOMES Program.

MULTIFAMILY INDIVIDUAL UNIT DATA ACCESS

In scenarios where a multi-family building has individual tenant meters for each unit, [STATE] will require the same authorization, notification, and revocation processes established for single-family buildings. This means utility account holders will have to affirmatively opt-in to having their energy usage data shared with a participating contractor, aggregators, and [STATE] and DOE.

It is important to note that in many circumstances an individual unit may be metered for one energy source but not all energy sources serving that unit (i.e., electricity, natural gas, etc.). In these scenarios, the [STATE] will need to pursue a hybrid approach.

MULTIFAMILY WHOLE BUILDING DATA ACCESS

[7] In the Home Energy Rebate program guidance ("Program Guidance"), DOE requires that states ``[e]nsure that any parties participating in a program that requires energy consumption data have secure data protection and protocols that demonstrate the capability for a safe transfer, of consumer data, including data for *individual dwelling units and whole-building aggregate data for multifamily buildings*."

In scenarios where a multi-family building has some combination of whole building metering, common area metering, and whole building tenant area metering, [STATE] will pursue a whole building data access strategy.

The whole building data access strategy seeks to "aggregate" the entire building's energy usage to enable participation in the HOMES or HEEHR program. This aggregation of a multifamily family's building data can be achieved through two distinct authorization, notification, and revocation processes.

In one pathway, a building owner or manager can authorize this data aggregation through a utility portal or a third-party tool like Energy Star Portfolio Manager without tenant authorization. However, this requires that a multifamily building exceed [STATE'S] aggregation threshold of X number of units or X% of units established by the [STATE PUC].

In the second pathway, a building owner or manager can authorize this data aggregation through a utility portal or a third-party tool like Energy Star Portfolio Manage, but only after receiving tenant authorization. This second pathway is less preferred due to the additional complexity but will be necessary to enable multifamily buildings below the [STATE's] aggregation threshold.

To enable multifamily properties of all sizes to participate in the HOMES and HEEHR programs, [STATE] will likely need to pursue both pathways.

EXCEPTIONS

The only instance in which an "opt-out" is used is in the case of sharing Portfolio Data, which by definition is not individually-identifiable.

CUSTOMER OUTREACH

[STATE plans to meet this DOE requirement: "States should describe how they will leverage multiple communication channels to effectively reach customers" (page 5, *Utility Data Access Guidelines*]

ELIGIBILITY AND ENFORCEMENT OF THIRD PARTIES

OVERSIGHT

If any entity working for [STATE], or an entity contracted to a vendor to [STATE], experiences a data breach, then [STATE] will investigate. Depending on the outcome of the investigation, that entity will be ineligible for state contracts. The entities directly contracted to the state are the ones responsible for data safety and security.

[LIST STATE BREACH NOTIFICATION LAWS OR PROCEDURES]

GREEN BUTTON ELIGIBILITY AND ENFORCEMENT

Any user of an electric or gas utility's GBC platform must agree to (1) the utility's terms and conditions and (2) requirements established by the Public Utility Commission. For electric or gas utilities not regulated by the Public Utility Commission (such as munis and co-ops), those utilities are encouraged to contact [STATE] if they have a reasonable suspicion that a data recipient has experienced a breach.

DATA AGGREGATION & ANONYMIZATION

[STATE] will employ aggregation and anonymization as appropriate for implementation of HOMES and HEERA in accordance with local laws. As such, we affirm that data control is in the hands of customers, except for primary use cases where consent may not be required. Derivative results at the portfolio level will be aggregated and anonymization will be employed as necessary in the program implementation processes to allow for disclosure only upon customer consent.

[STATE]'s approach to aggregation and anonymization is grounded in the Fair Information Practice (FIP) Principles, developed by the FTC in the 1970s, and later adopted by the Department of Homeland Security. Utilities and third parties with appropriate security credentials may be authorized custodians of the data on behalf of (consenting or non-consenting) customers. They hold the liability to protect the privacy of the customer. As such, custodians of the data may have access to identifiable information such as customer usage and other metadata that enhance that data's usefulness and offer potential insights that would otherwise be unavailable.

Data custodians are required to protect data to ensure data is non-identifiable (back to the customer) by anonymizing and/or aggregating data sets that are not obtained via customer consent. They will ensure the processes and formats to share data and get customer consent are secure. They may be enabled with standards like GBC.

Our [STATE] data access framework utilizes a risk-based approach to assess data access and follow the general security guidelines in place in [STATE] for energy consumption data.

Aggregation thresholds are a common practice to protect customer privacy. For this use case, aggregation would only need to apply in presenting energy savings results and program impacts to the public agency and in reporting to DOE. Since the data set reported to DOE must be disaggregated and only includes information obtained with customer consent [STATE] will not adopt an aggregation threshold except for publicly posted derivative portfolio results. [OR] To provide additional privacy protection to participants, [STATE] adopts a binary aggregation threshold of a 10-customer [or pick another number] minimum in any portfolio and results will be anonymized so participating individuals cannot be re-identified. Given the homogeneity of residential populations, the risk of individual re-identification is limited and the potential harm from release is negligible.

MULTI-FAMILY WHOLE-BUILDING AGGREGATED DATA

[STATE paste EnergyStar process for each utility with the applicable aggregation threshold]

QUALITY AND ACCESSIBILITY OF ENERGY USAGE DATA

INTRODUCTION

[STATE]'s treatment for each data source in terms of its level of quality or authoritativeness, and how the accuracy and integrity of information is maintained during transmission, is described in the table below.

DATA SOURCE	QUALITY TREATMENT	ENSURING ACCURACY DURING TRANSMISSION
Electric or gas utilities (whether via utility bills or spreadsheets via email)	Assumed to be high quality. No further verification is required because the utility is presumed to have ensured its validity.	.
Interval energy usage data provided by electric or gas utilities via GBC		Since TCP/IP is used, including Secure Socket Layers (https), the accuracy and integrity of energy usage information during transit is assured
Delivered fuel paper records	Assumed to be high quality, no further verification is required	N/A
Delivered fuel sensors	The monitored fuel oil consumption will be compared to delivered fuel records to validate accuracy.	Since TCP/IP is used, including Secure Socket Layers (https), the accuracy and integrity of energy usage information during transit is assured.

DELIVERED FUELS AND USING SENSORS FOR PROPANE SYSTEMS

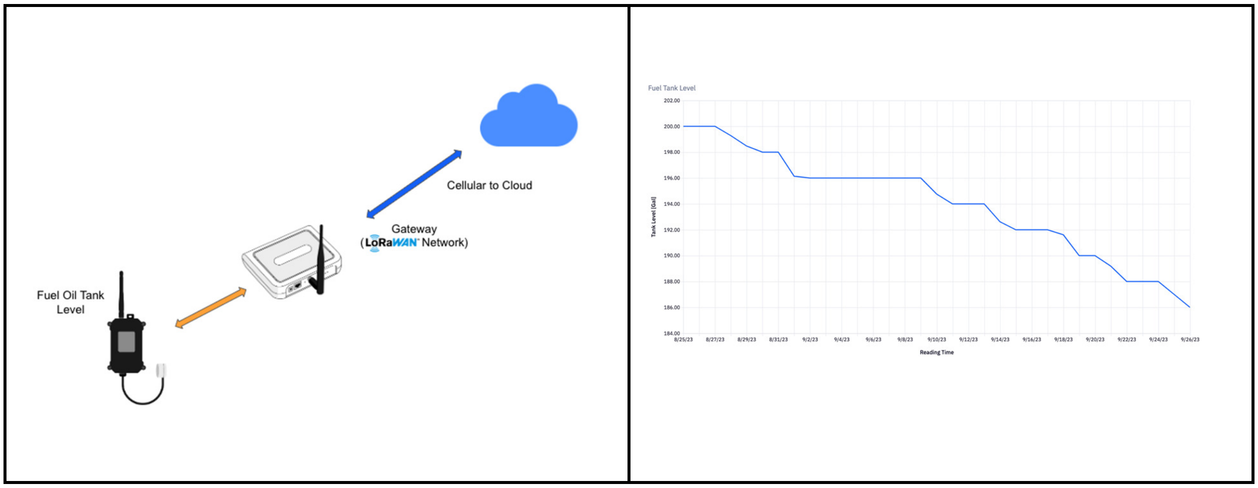
Delivered fuels, such as fuel oil and propane, are inherently more difficult to track usage than metered fuels like electricity and natural gas. Deliveries may come only every 1 - 4 months, and often the only record is the paper bill left by the delivery company. This means usage data is less granular and timely, especially if measuring the impacts of energy efficiency upgrades after projects are completed.

One approach to solving this issue is to leverage easy-to-install, battery-powered sensors that measure tank levels every 15 minutes, every hour or once-a-day depending on the use case. This granular and continuous data enables households, Contractors, Program Implementers, and others to measure energy usage and savings for space heating, water heating, cooking and more. These sensors are typically installed by Contractors in about 15 - 30 minutes.

There are several wireless technology options available on the market today, providing optionality for users. In general, (1) the sensors measure the change in the level of fuel in the tank, (2) communicate this data wirelessly to a hub (also called a gateway), and (3) the gateway streams the data to the cloud in real time. One common solution uses Long Range Wireless Area Network (LoRaWAN) technology, which enables sensors to communicate across large homes and multifamily buildings, have batteries that last 5 to 10 years, and do not utilize local WiFi or ethernet.

***Optional Images to support delivered fuels section**.*

Figure X. Example of wireless sensor devices for measuring fuel oil tank levels; chart showing tank level changes by day



HANDLING DISCREPANCIES

The quality and accuracy of incoming energy usage data will be key in successful [STATE]'s program delivery. [STATE] will establish protocols to identify and rectify discrepancies, which is essential to ensure data reliability. This section outlines the key considerations we will incorporate into our procedures, and identifies common discrepancies encountered and [STATES]'s steps for resolution.

Key considerations:

- **Source Verification**: Ascertain the source of incoming data. While utilities are primary contributors, data may also come from data managers, third-party providers, or customer-owned devices.
- **Frequency and Granularity**: Identify discrepancies in data granularity (e.g., hourly vs. daily) and ensure consistency in the frequency of data updates.
- **Data Gaps**: Detect missing data points or periods without data, which can disrupt analysis.
- **Outliers**: Identify data points that deviate significantly from typical patterns or historical trends.
- **Validation Against Known Patterns**: Compare incoming data against established patterns or baselines, flagging unexpected deviations.
- **Data Integrity**: Ensure that data has not been altered or tampered with during transmission or storage.

Possible discrepancy types are shown below along with their treatment. The table below has been informed by CalTRACK v2.0's methods concerning data management.[8]

TYPE OF DISCREPANCY	TREATMENT
Obvious utility billing error	Review the bill for anomalies like sudden spikes in usage or charges. Engage with the utility for verification and correction.
Inconsistent Granularity	Standardize data granularity to a common format, e.g., converting hourly data to daily averages if needed.
Missing Data Points	Engage with the data source to fill gaps. Use interpolation methods if source data is unavailable.
Outliers	Review and validate extreme data points. If genuine, investigate the cause. If erroneous, seek corrections from the data source.

[8] https://docs.caltrack.org/en/latest/methods.html#section-2-data-management

Unusual Patterns	Validate against historical trends or expected patterns. Discuss potential reasons with the utility or data provider.
Data Tampering or Alteration	Implement secure transmission and storage protocols. Periodically verify data integrity against trusted backups.

With regard to modeled savings, [STATE] will follow the data exception handling procedures outlined in BPI 2400 Section 3.2.2 “Model Calibration Utility Bill Criteria.” These procedures cover topics such as handling estimated utility readings and having at least 330 days of energy usage reflected in utility bills.

CONCLUSION

[ANY FINAL THOUGHTS OR CONCLUSIONS ON THE STATE’S APPROACH]