Appendix Index

Appendix A

AGO Proposed Rule

Rule R8-51. CUSTOMER AND THIRD-PARTY DATA ACCESS AND PRIVACY.

(a) Definitions.

(1) "Aggregated data" means usage data or energy savings data at a premises from which no individual, family, household, residence or customer could be identified or reidentified with reasonable effort in the judgment of the transferor if such data were made public. Before transferring any aggregated data, a transferor shall:

(i) Remove all information that could identify any particular individual, family, household, residence or customer;

(ii) Combine and/or process the data with the data of a sufficiently large group of customers in the manner described by this Rule; and

(iii) In appropriate cases, utilize other anonymization techniques. Such techniques may include, without limitation, reducing the granularity of the data transferred or differential privacy.

(2) "Application programming interface" or "API" means a utility's internet-based system that securely provides customer data to customer-authorized third-parties using machine-to-machine communications.

(3) "Authorized third party" means a third party that has received authorization from a customer to access, receive, collect, store, use, or disclose standard customer data and that obtains the information from a utility.

(4) The "Commission" is the North Carolina Utilities Commission.

(5) "Covered information" means any information that is "standard customer data," "unshareable personal data," or "usage data" as defined in this rule. Covered information does not include, however, aggregated data. Covered information also does not include information provided to the Commission pursuant to its oversight responsibilities.

(6) "Electric Services Purposes" means purposes relating to Commission-regulated electric power generation, transmission, distribution, delivery, and sales, and other regulated services, including, but not limited to, administration of customer accounts and rate schedules, metering, billing, standby service, backups, and changeovers of service to other suppliers.

(7) "Secondary purpose or use" means any purpose or use that is not an electric services purpose or use.

(8) "Standard customer data" means

(i) all energy usage data collected by a meter that a utility maintains as part of its regular records in the ordinary course of business, including kilowatt-hours used, load profile, and, where applicable to certain rate classes, kilo-volt-amps, kilo-volt-amperes-reactive, power factor, and the like;

(ii) customer-specific information including customer name, mailing address, premise address, any contact information, payment history, account number(s), and all information on bills including, but not limited to, line item charges and charge descriptions, amounts billed, the rate or tariff applicable to the account or meter, billing cycle dates, etc.; and

(iii) any information that might be necessary for participation in, or to determine customer eligibility for, bill payment assistance, renewable energy, demand-side management, load management, or energy efficiency programs**.**

Standard customer data does not include unshareable personal data.

(9) "Unshareable personal data" means the birth date, social security number, biometrics, bank and credit card account numbers, driver's license number, credit reporting information, bankruptcy or probate information, health information, or network or internet protocol address of the customer or any person at the customer's location. This personal information is specifically excluded from the definition of standard customer data and, as stated in subdivision (d)(9) of this Rule, will not be shared by a utility with any party other than the customer.

(10) "Usage data" is all energy usage data collected by a meter including but not limited to kilowatt-hours used, load profile, kilo-volt-amps, kilo-volt-amperes-reactive, power factor, kW, or voltage.

(11) For purposes of this rule, the word "utility" has the same meaning as is defined in Rule R8-2.

(12) For purposes of this rule, a "utility contractor" means any third party that provides services to a utility under contract with that utility.

TRANSPARENCY (NOTICE OF USE OF CUSTOMER INFORMATION)

(b) Notice.

(1) Generally. – Utilities shall protect covered information in their possession or control to maintain the privacy of customers. Utility contractors' permissible uses of data and obligations to protect data are governed by contract with the utility as set forth in subsection (d) of this rule.

(2) Notice Requirement. – Utilities shall provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the accessing, collection, storage, use, and intentional disclosure of covered information. Utilities shall also provide such notice regarding the compilation, use, and disclosure of aggregated data.

(3) When Provided. – Utilities shall provide a written notice that meets the requirements of subdivision (b)(2) when confirming a new customer account, and at least once a year, utilities shall inform customers how they may obtain an updated copy of this notice. Utilities shall provide a conspicuous link to such notices under subdivision (b)(2) on the home page of their websites. Moreover, utilities shall include a link to the notice in all electronic mail to customers. Utilities shall also provide this notice upon request by any party.

(4) Form. – The notice, which may take the form of or be included in a privacy policy, shall be labeled "Notice of How We Gather, Use and Disclose Your Information" and shall:

(i) Be written in easily understandable language; and

(ii) Be no longer than is necessary to convey the requisite information.

(5) Content. – The notice shall state clearly:

(i) The identity of the utility;

(ii) The effective date of the notice;

(iii) The utility's process for altering the notice, including how the customer will be informed of any alterations and where prior versions will be made available to customers; and

(iv) The title and contact information, including email address, postal address, web address, and telephone number, of an official at the utility who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or disclosure of covered information or aggregated data.

The notice shall also:

(v) Include a description of the standard customer data made available to customers;

(vi) Indicate the frequency with which standard customer data can be provided;

(vii) Explain that disclosure of customers' data to third parties affects customer privacy, providing insight into their energy-consuming behaviors and permitting inferences about customers' daily activities, absences from the home or business, patterns of behavior, and lifestyle;

(viii) Explain that customers, before they authorize the disclosure of their data to third parties, should consider how the third party would be able to access and use their data;

(ix) Explain that the privacy and security of customer account and usage data will be protected by the utility while the data is in the utility's possession or control, but that the utility is not responsible for the privacy or security of the data after it has been transferred successfully to the customer or to an authorized third party;

(x) Identify any charges that may be applicable for customers to access data that are not standard customer data;

(xi) State that standard customer data will not be disclosed to third parties without customers' express, written consent in a manner and form approved by the Commission;

(xii) Explain the utility's policies regarding the manner in which a customer can authorize access and disclosure of covered information to third parties;

(xiii) Describe how the customer can terminate authorized third-party access to covered information;

(xiv) Inform customers that, unless they opt out, covered information will be used to create aggregated data reports that will not contain customer-identifying information, that the utility may provide such aggregated data to third parties, and that covered information may be shared confidentially with researchers subject to Commission Rule R8-51;

(xv) Provide information about how a customer may opt out of the aforementioned use of their covered information; and

(xvi) Explain that unshareable personal information will not be shared by a utility with any party other than the customer at any time.

(c) Purpose Specification. – The notice required under subsection (b) shall also provide:

(1) An explicit description of:

(i) Each category of covered information collected, used, stored or disclosed by the utility, and, for each category of covered information, the reasonably specific purposes for which it will be collected, stored, used, or disclosed.

(ii) Each category of covered information that is disclosed to third parties, and, for each such category:

(a) The purposes for which it is disclosed; and

(b) The categories of third parties to which it is disclosed.

(iii) The specific identities of those authorized third parties to whom data is disclosed for secondary purposes, and the secondary purposes for which the information is disclosed.

(2) The approximate period of time that covered information will be retained by the utility or utility contractor.

(3) A description of:

(i) The means by which customers may view, inquire about, or dispute their covered information; and

(ii) The means, if any, by which customers may limit the collection, use, storage or disclosure of covered information and the consequences to customers if they exercise such limits.

USE AND DISCLOSURE LIMITATION

(d) Use and Disclosure Limitations.

(1) Generally. – Utilities are authorized to use covered information to provide regulated utility service for Electric Service Purposes.

(2) No Sale of Customer Information. – Utilities may not sell information about customers, covered information, or aggregated data. However, utilities may require payment of approved charges and fees in the manner set forth by this Rule.

(3) Use of Covered Information by a Utility for Electric Service Purposes. – A utility may access, collect, store and use covered information without customer consent, provided the use is for Electric Service Purposes and no disclosure is made to a utility contractor except as allowed by subdivision (d)(4) below.

(4) Disclosure by a Utility Without Customer Consent. – A utility may disclose standard customer data to a utility contractor without customer consent only:

(i) When explicitly ordered to do so by the Commission; or

(ii) For a primary purpose being carried out under contract with and on behalf of the utility disclosing the data; provided that the utility shall, by contract, require the utility contractor to agree to use the data only for the primary purpose and to access, collect, store, use, and disclose the information pursuant to policies, practices and notification requirements no less protective than those under which the utility itself operates as required under this rule, unless otherwise directed by the Commission. As part of this contractual agreement, utilities shall require utility contractors to provide similar contractual protections for standard customer data in the context of all subsequent disclosures for Electric Service Purposes.

(5) Terminating Disclosures to Entities Failing to Comply With Their Privacy Assurances. – When a utility discloses standard customer data to a utility contractor under this subsection (d), it shall specify by contract, unless otherwise ordered by the Commission, that it shall be considered a material breach if the contractor engages in a pattern or practice of accessing, storing, using or disclosing the information in violation of the party's contractual obligations to handle the information pursuant to policies no less protective than those under which the utility from which the information was initially derived operates. If a utility determines in good faith that a utility contractor is in breach of its contract for this reason, the utility shall promptly cease disclosing the information to the contractor.

(6) Ban on Disclosure for Secondary Purposes Without Consent. – No utility shall use or disclose standard customer data to any party for any secondary purpose without obtaining the customer's prior, express, voluntary, authenticated authorization for each distinct secondary purpose. This authorization is not required when information is:

(i) Provided pursuant to a legal process;

(ii) Provided in situations of imminent threat to life or property;

(iii) Specifically authorized by the Commission pursuant to its jurisdiction and control; or

(iv) Otherwise expressly permitted by this Rule.

(7) Requirements for Authentications of Consent. – Customer

authorizations to disclose customer data are authenticated, under this Rule, if the customer's identity is established in either oral, electronic or non-electronic form and can be documented by the utility. Separate authorization by each customer must be obtained for all secondary uses of covered information by a utility.

(8) Form of Consent. – The customer consent form or process must be approved by the Commission, and shall include:

(i) Information to adequately identify the customer, consistent with, and no more onerous than, a utility's authentication practices when a customer creates an online account on a utility's website or when a customer calls the utility by telephone;

(ii) The intended purpose and the use of the data being requested;

(iii) The time period (e.g., months, years) during which the secondary use will take place;

(iv) The category of information to be shared, with a succinct description of each; and

(v) In the event a utility seeks to use customer data for a secondary purpose, a commitment to the customer that the utility shall be responsible for using the data only for the authorized secondary use and that the utility will continue to protect the privacy and security of the data in accordance with this rule.

If a consent is made by electronic means, the information provided shall be in spoken form, displayed on a screen, or otherwise displayed to the customer via the customer's preferred contact method. If a consent is made by oral means, the information listed in sub-subdivisions (i) through (iii) shall be obtained and provided in spoken form, but the commitment to the customer in sub-subdivision (iv) may be provided either in spoken form or by directing the customer to a website that provides the commitment to the customer.

(9) Ban on Disclosure of Unshareable Personal Data. – Nothing in this Rule shall allow, and utilities shall be prohibited from, providing unshareable personal data to any party other than the customer. However, network or internet protocol addresses may be shared by a utility to a utility contractor for an electric services purpose.

CUSTOMER ACCESS AND CONTROL

(Individual Participation)

(e) Customer Access and Control.

(1) Quality and Quantity of Standard Customer Data. – A utility shall maintain at least 24 months of standard customer data, or the period of time that a customer has had an account at a given address, whichever is less, in sufficient detail for a customer to understand his or her energy usage. The frequency interval of data must be commensurate with the capabilities of the meter or network technology used to serve the customer.

(2) Customer Access to Standard Customer Data. – As part of basic utility service, upon request, a utility shall provide a customer access to the customer's own standard customer data provided in electronic machine-readable format, in conformity with nationally recognized standards and best practices concerning form and frequency, such as the latest version of the North American Energy Standard Board's (NAESB) Req. 21, the Energy Services Provider Interface (ESPI), and in a manner that ensures adequate protections for the utility's system security and the continued privacy and security of the customer data during transmission.

(3) Cost. –When the data requested is standard customer data, is authorized by the customer, and the request pertains to a time period within the previous 24 months, the request for access will be fulfilled without charge. If requests are made for information other than standard customer data or data outside the 24 months preceding the request, and utilities seek to charge customers a fee to provide such data, the utility may charge an amount that the Commission deems reasonable based on the utility's marginal cost to provide those data.

(4) Control. – Customers have the right to share their own standard customer data with authorized third parties of their choice to obtain services or products provided by those third parties and to ensure accuracy of covered information held by utilities and utility contractors. Utilities shall provide customers with convenient mechanisms for:

(i) Granting and revoking authorization for secondary uses of standard customer data by third parties;

(ii) Disputing the accuracy or completeness of any covered information that a utility is storing or distributing for any primary or secondary purpose; and

(iii) Requesting corrections or amendments to any covered information that the utility is collecting, storing, using, or distributing for any primary or secondary purpose.

AUTHORIZED THIRD PARTY ACCESS

TO CUSTOMER DATA FROM A UTILITY

(f) Authorized Third Party Access to Standard Customer Data from a Utility.

(1) Third Party Access upon Customer Authorization. – For the period of time during which a customer has provided consent, utilities shall grant authorized third parties access to the customer's standard customer data in electronic machine-readable format, in conformity with nationally recognized standards and best practices concerning form and frequency, such as the latest version of the North American Energy Standards Board's (NAESB) Req. 21, the Energy Services Provider Interface (ESPI), and in a manner that ensures adequate protections for the utility's system security and the continued privacy of the data in transit from a utility to an authorized third party. Following receipt of a valid customer authorization as described below, utilities shall electronically initiate requested data to the third party within 90 seconds, unless the customer has requested data delivery by another method.

(2) Customer Authorization. – Utilities shall designate the categories of standard customer data available to authorized third parties in conformity with this rule and provide brief descriptions of those categories in plain language for customers to understand. For all methods of authorization described below, when a customer authorizes third party access, the customer will identify the categories of information the customer wishes to share. If an authorized third party specifies the data it would like permission to access, the utility shall display such request to customers using the aforementioned categorical designations. Separate authorization by each customer must be obtained for all disclosures of standard customer data except as otherwise provided for herein.

(3) Authorization Process. – A utility shall not disclose standard customer data to a third party unless an authorization is valid as described in this rule. A utility shall, regardless of the authorization method described in this Rule, use consistent customer information to validate the customer's identity in a manner that is no more onerous than a utility's authentication practices when a customer creates an online account on a utility's website or when a customer calls the utility by telephone. A utility shall provide the following methods for any customer to grant a valid authorization: non-electronic; customer-initiated electronic; and at least one authorized third-party initiated electronic method using an API that is non-proprietary to the utility and is commonly used in the industry by other utilities. In addition, a utility shall provide additional customer-requested authorized third-party initiated electronic methods described below subject to its capability to do so without substantial additional cost.

(i) Non-electronic methods. Any customer may submit an authorization to a utility by at least the following methods:

(a) By telephone, in which authorizations shall be processed, and data transmitted, within one (1) business day; or

(b) By mail to a utility's mailing address, in which case authorizations shall be processed, and data transmitted, within one (1) business day.

(ii) Customer-initiated electronic methods. Any customer may submit an authorization to a utility by completing a web-based submission on a utility's website, consistent with nationally recognized standards and best practices. In this case, a utility shall allow direct online submission following completion without requiring email or an online account.

(iii) Customer-requested, authorized third party initiated electronic methods. A customer may interact directly with a third party and provide the third party with the customer's account number. The utility shall receive a customer's account number from the third party via API and seek authentication from the customer as well as customer consent via the customer's preferred contact method (such as by one-time passcode). Once authorized, the utility shall provide the requested data to the authorized third party via API. In this context, the utility will authenticate the customer's identity, process the request for access, and permit electronic authorization via API in a timeframe no longer than the time required for a customer to create an online account at a utility's website and access his or her standard customer data.

(4) Requirements of authorization. – For all authorization methods used, a utility shall

(i) Enable and require the designation of the authorized third party and the customer;

(ii) Enable and require the specification of the purpose for sharing the data and the intended use of the data by the authorized third party;

(iii) Enable and require the designation of the time period (e.g., months and years of both historic and future data) for which data is being requested. The utility shall provide customers the option to authorize an ongoing provision of data that is valid until revoked by the customer or provision for a specified period of time.

(iv) Enable and require the designation of the categories of standard customer data being requested in accordance with subdivision (f)(2).

(v) Provide notice to the customer that, following access or transfer, the utility shall not be responsible for monitoring or ensuring that the third party to whom the data is disclosed is maintaining the confidentiality of the data or using the data as intended by the customer.

(5) Revocation and Termination. – Customers have the right to revoke, at any time, any previously granted authorization. Termination of electric utility service also terminates consent to disclose customer data granted by the customer for the meter(s) or premise(s) where electric utility service has been terminated. A utility shall also permit an authorized third party to terminate its authorization, in which case a utility shall subsequently notify a customer of the termination via the customer's preferred contact method and confirm to the authorized third party that the termination is accepted.

(6) Opportunity to Revoke. – The consent of a residential customer shall continue without expiration if the customer has elected ongoing provision until revocation, but the utility must contact a customer once annually to inform the customer of the authorization(s) granted and to provide an opportunity for revocation. The utility shall use electronic means to make this annual notice if the utility holds electronic contact information for the customer. The consent of a non-residential customer shall continue in the same way, but a utility must notify a non-residential customer once, upon an initial authorization, to provide an opportunity for revocation.

(7) Modifications. – Changes of contact names for an organization, trade name, or utility over time do not invalidate consent as to the respective organization, trade name, or utility. Modifications to the consent form or process over time do not invalidate previous consent.

(8) Parity. – Utilities shall permit customers to revoke authorization for any secondary purpose of their standard customer data by the same mechanism(s) initially used to grant authorization.

(9) Eligibility Determinations. – To protect the privacy and security of covered information, utilities shall apply eligibility criteria as follows. To be eligible to receive standard customer data, authorized third parties shall be required by utilities to: (i) demonstrate technical capability to interact securely with the utility's servers; (ii) provide contact information and federal tax identification numbers to a utility; (iii) acknowledge receipt and review of these privacy and access Rules; (iv) not have been disqualified as an authorized third party provider in the past pursuant to processes outlined at subdivisions (h)(2)-(4); and (v) adopt and comply with the most updated

version of the 2015 Department of Energy's Voluntary Code of Conduct Final Concepts and Principles for Data Privacy and the Smart Grid (the "DataGuard Seal") or a similar nationally accepted eligibility standard approved by the Commission as a necessary, comparable, reasonable and appropriate alternative.

(10) Descriptive rate schedules. – A utility shall include in its rate schedules a description of standard customer data that it is within the utility's technological and data capabilities to provide to the customer, to an authorized representative of the customer, or to an authorized third party recipient. At a minimum, the utility's rate schedule must provide the following:

(i) A description of standard customer data and the frequency of updates that will be available;

(ii) The method and frequency of standard customer data transmittal and access available (electronic, paper, etc.), pursuant to which data is provided to authorized third parties as soon as practicable following collection of the usage data, as well as the security protections or requirements for such transmittal;

(iii) A reasonable timeframe for processing requests, consistent with this rule; and

(iv) Any fees or charges associated with processing a request for usage data.

(11) Records of Disclosures. – The utility shall maintain records of all disclosures of covered information to third parties, including a copy of the customer's authorization to disclose standard customer data (unless it was in oral form) and a list of the information disclosed using the categories developed by the utility under subdivision (f)(2) of this Rule. The utility shall maintain records of standard customer data disclosures for a minimum of three years and shall make the records of the disclosure of a customer's data available for review by the customer upon request.

LIABILITY AND COMPLAINTS

(g) Liability. – Nothing in this Rule shall be construed to impose any liability on a utility or any of its directors, officers and employees, relating to disclosures of information when (1) the Commission orders the provision of standard customer data to a third party; or (2) a customer discloses covered data to, or authorizes access to standard customer data by, a third party that is unaffiliated with and has no other business relationship with the utility. Specifically, after a utility securely transfers covered information to a customer or standard customer data to an authorized third party pursuant to a customer's request,

nothing in this Rule shall make a utility responsible for the security of the information or its use or misuse by such customer or by a third party. This section does not apply where a utility has acted recklessly.

(h) Complaints.

(1) Complaints Submitted by Customers Against Utilities. Complaints from customers regarding a utility's failure to process customer authorizations to release standard customer data pursuant to this Rule in a timely and accurate manner, or to provide eligible authorized third parties with access to a customer's standard customer data in a timely and accurate manner, or regarding the utility's failure to comply with this Rule in any other respect, shall be treated as complaints under Rule R1-9.

(2) Complaints Submitted to a Utility. If a utility disclosing standard customer data to a Commission-authorized or customer-authorized third party receives a customer complaint about the third party's misuse of data, the utility shall keep records of such complaints and submit a report to the Commission annually of any such complaints or suspected violations. If a utility believes it is necessary to terminate an authorized third party's access to customer data, the utility shall file a request with the Commission in accordance with subdivision (h)(3).

(3) Complaints submitted by a utility. If a utility has a reasonable suspicion that an authorized third party has engaged in conduct rendering it ineligible to access information under this Rule, the utility shall expeditiously inform the Commission and the Public Staff of any information regarding possible ineligibility.

(4) If the Commission confirms that a third party is or has become ineligible to receive information as an authorized third party under this Rule, the Commission shall allow the utility to refrain from providing or to discontinue providing standard customer data to that party.

A utility will not be deemed to have made a reckless transmission of covered information to an authorized third party if the utility acts consistently with the process described in subdivisions (2) and (3) above.

A utility is prohibited from unilaterally revoking access to an authorized third party for any reason other than a Commission order pursuant to paragraph 4 above or a good faith belief that the third party poses an imminent danger to life, property or the cybersecurity of the utility's systems.

(i) Penalties. – An admission to or Commission adjudication of liability for a violation of these rules may result in an assessment of a civil penalty or fine as provided by 15 N.C. Gen. Stat. § 62-310 et seq.

AGGREGATED DATA

(j) Aggregated Data.

(1) Availability of Aggregated Data. – Utilities may permit the use of aggregated data from which all identifiable information has been removed to be used for analysis, reporting or program management provided that the release of that data does not disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information.

(2) Requests for Aggregated Data. Unless otherwise specified below, individual customers need not consent to requests for aggregated data in the following circumstances. If the requirements below are not met, then the requestors must secure and provide the utility evidence of explicit authorization from each customer whose usage data are subject to the request.

(i) Publicly Available Aggregated Data. A utility must make the following types of data available on its public website:

(a) Usage data showing the total amount of energy used in one calendar year within the State of North Carolina, the utility, any municipality, any zip code, any census block group, or any census block. These data shall be posted as close to real-time as possible.

(b) Usage data showing the total amount of energy used in any quarter in the State of North Carolina, the utility, any municipality, any zip code, any census block group, or any census block. These data shall be updated at least once every six months.

(c) Usage data showing the total amount of energy used in any calendar month by the State of North Carolina, the utility, or a municipality. These data shall be updated at least once every six months.

(d) Usage data showing the total amount of energy used in any increment of time collected by the utility within the State of North Carolina. These data shall be updated at least once every six months.

(e) With respect to aggregated data for any municipality, the utility or the State of North Carolina, the utility shall provide such data with whether the usage is residential or nonresidential. These data shall be updated at least once every six months.

(ii) EnergyStar. If a requestor seeks aggregated data for a particular building or premises owned or operated by that requestor for the purposes of obtaining United States Environmental Protection Agency's EnergyStar certification or ranking, or complying with a

law, ordinance or regulation related thereto, then a utility shall timely fulfill requests for aggregated data for that particular building or premises if the requirements below are met.

(a) *Only Monthly, Whole-Building Data in Usable Format.* The provided aggregated data shall consist only of monthly, whole-property consumption data for the requested building or premises. The utility shall provide updated data each month, if so requested, and in accordance with any best-practices document promulgated by the United States Environmental Protection Agency.

(b) *Residential or Commercial Units Only*: If the building or premises subject to the data request contains only residential units, commercial units, or a combination thereof, the requested usage data will be considered aggregated data if (1) all identifying information has been removed and (2) there are at least four customers, and no single customer's energy use equals or exceeds 50% of the total energy use in any given month.

(c) *Industrial Units*: If the building or premises contains any industrial units, the requestor must obtain the consent of the customers before obtaining aggregated data.

(d) If the aggregated data are being provided without customer consent, the recipient must enter into a nondisclosure agreement with the utility. That agreement must specify, at a minimum, that:

1. the requestor may use the aggregated data only for the purposes of building benchmarking, identifying energy efficiency projects, and energy management and complying with local laws and ordinances;
2. the requestor will not identify or reidentify any individual customers;
3. the requestor shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure; and
4. the requestor may not transfer the data to any other party, other than a third party who agrees not to transfer the data further and to abide by the other terms above.

(iii) Academic Researchers and Government Entities: Aggregated Data from Utility. – In addition to the publicly available aggregated data above, academic researchers and government entities may obtain the aggregated data from a utility subject to the following terms:

(a) The following types of aggregated data will be made

available:

1. Aggregated data showing the amount of energy used in one calendar month by any zip code, census block group, or census block per rate class.
2. Aggregated data showing the amount of energy used in one day by any municipality, zip code, census block group, or census block per rate class.
3. Aggregated data showing the amount of energy used in any increment of time longer than 15 minutes by any municipality or zip code per rate class.

(b) An academic researcher or government entity shall execute a nondisclosure agreement in a form approved by the Commission. That nondisclosure agreement shall provide:

1. the recipient may use the usage data only for the purposes of studying energy;
2. the recipient party may not transfer any usage data to any other party;
3. the recipient will not identify or reidentify any individual customers; and
4. the recipient shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure, including that the usage data shall be destroyed after it has been used for the purposes of the program.

(iv) Public University Repository. – A public institution of higher education in North Carolina ("public university") may obtain two years' usage data together with the address of record and rate class with no other personally identifying information from a utility for no financial consideration. A public university receiving such usage data may obtain updated usage data every six months. A person who wishes to obtain aggregated data not otherwise available under this rule may request the data from the public university. The public university shall be required to execute a nondisclosure agreement with the utility in a form approved by the Commission. That nondisclosure agreement shall include at least the following terms:

(a) Implement commercially reasonable data security and cybersecurity measures including, but not limited to, physical and technical safeguards, limiting the number of people who may have access to such data to those with a need for such data, in addition to any safeguards that may

be required by the institutional review board of the Public University.

(b) The public university may use the usage data only for academic, research or policy purposes. It may not use the usage data for purely commercial purposes.

(c) The public university may choose to provide aggregated data to third parties. That aggregated data must be either (1) otherwise available to the third party under this rule (e.g., publicly-available aggregated data) or (2) stripped of any personally-identifying information and anonymized using privacy-enhancing techniques, such as differential privacy, in a manner sufficient to prevent reidentification. The recipient must execute a nondisclosure agreement and agree to use the data only for energy-related purposes, not to transfer the data to any other party, and not to attempt to reidentify any particular individual, family, household, residence or customer.

(d) The public university may not provide aggregated data to a third party if (1) the aggregated data reveal specific customer information because of the size of the group, rate classification, or nature of the information or (2) the aggregated data otherwise contain identifiable critical infrastructure or other sensitive data that should not be disclosed for security or, in the public university's view, extreme confidentiality purposes.

(e) In the event that the Public University or a party to whom the Public University provides any data publishes or otherwise provides information obtained from processing the data, any such publications or provisions shall not provide enough information to permit reidentification of any individual, family, household, residence or customer without extraordinary effort.

(f) The public university shall notify the Commission of any breach with respect to the usage data, and the Commission shall have audit rights over the public university's use of the data and may delegate those audit rights to other parties. The Commission may, in its discretion, cut off or reduce the public institution of higher education's access to the usage data if the Commission finds that it is not abiding by the terms of the nondisclosure agreement or this Rule.

(g) The public university shall be subject to reasonable data minimization and data retention policies.

(v) All requests for aggregated data shall be treated in accordance with the rate schedules to be filed pursuant to sub-subsection (j)(4). Such rate schedules may include additional categories of aggregated data not explicitly referenced in this rule. In the event

no rate schedules that concern aggregated data have been filed, the utility shall nevertheless process requests for the categories of aggregated data explicitly mentioned in this rule as set forth herein.

(vi) In the event that any provision concerning restrictions on the transfer of aggregated data without customer consent are deemed unlawful, this Rule shall be interpreted to provide the maximum protection against sharing or usage of the aggregated data without customer consent.

(3) Opportunity to Revise Requests. – If an aggregated data report cannot be generated in compliance with this rule, the utility shall notify the requestor that the aggregated data, as requested, cannot be disclosed and identify the reasons the request was denied. The requestor shall be given an opportunity to revise its aggregated data request in order to address the identified reasons.

(4) Rate Schedules. – A utility shall file for Commission approval to amend its rate schedules to include a description of aggregated data reports available from the utility. At a minimum, the utility's rate schedules shall provide the following:

(i) A description of the aggregated data reports available from the utility, including all available selection parameters (usage data or other data);

(ii) The frequency of data collection;

(iii) The method of transmittal available (electronic, paper, etc.) and the security and privacy protections or requirements for such transmittal;

(iv) The applicable charges for providing an aggregated data report;

(v) The timeframe for processing requests; and

(vi) A form for requesting an aggregated data report to the utility identifying any information necessary from the requestor in order for the utility to process the request.

(5) Optouts. A customer may opt out of its data being provided to other parties under this subsection (j). In such a case, the utility shall not provide such customer's information to any other party.

(6) Any data a utility provides pursuant to this subsection (j) shall be provided in accordance with any best practice guidelines provided by the United States Environmental Protection Agency, with respect to EnergyStar-related data, as provided above, or the United States Department of Energy,

with respect to any other data, within 90 days of the guidelines being promulgated.

REPORTING ON DISCLOSURES PURSUANT TO LEGAL PROCESS

(k) Disclosure Pursuant to Legal Process.

Except as otherwise provided in this rule, a court order, state or federal law, or by order of the Commission:

(1) Reporting. – On an annual basis, utilities shall report to the Commission the number of demands received for disclosure of customer data pursuant to legal process and the number of customers whose records were disclosed. Upon request of the Commission, utilities shall report additional information to the Commission on such disclosures. The Commission may make such reports publicly available without identifying the affected customers unless making such reports public affects or would affect an ongoing criminal investigation.

DATA MINIMIZATION

(l) Data Minimization, Generally. – Utilities shall collect, store, use, and disclose only as much covered information as is reasonably necessary or as authorized by the Commission to accomplish the reasonably specific primary purpose identified in the notice required under subsections (b) and (c) or for a specific secondary purpose authorized by the customer.

(m) Data Retention. – Utilities shall maintain covered information only for as long as reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under subsections (b) and (c) or for a specific secondary purpose authorized by the customer.

(n) Data Disclosure. – Utilities shall not disclose to any third party more standard customer data than is reasonably necessary or as authorized by the Commission to carry out a specific primary purpose identified in the notice required under subsections (b) and (c) or for a specific secondary purpose authorized by the customer.

DATA QUALITY AND INTEGRITY

(o) Data Quality and Integrity. – Utilities shall ensure that covered information they collect, store, use, and disclose is reasonably accurate and complete or otherwise compliant with applicable rules and tariffs regarding the quality of energy usage data.

DATA SECURITY

(p) Data Security and Breach Notification.

(1) Generally. – Utilities shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

(2) Notification of Breach. – Notwithstanding and in addition to any other legal requirements, a utility shall require a utility contractor providing services to a utility for a primary purpose to notify the utility that is the source of the data within 24 hours (or, if in the utility's judgment a greater amount is necessary, 72 hours) of the detection of a security breach. Upon a security breach affecting 1,000 or more customers, whether by a utility or by a third party described herein, the utility shall notify the Commission of security breaches of covered information within two weeks of the detection of a security breach or within one week of notification by a third party of such a breach. Upon request by the Commission, utilities shall notify the Commission of security breaches of covered information.

(3) Annual Report of Breaches. – In addition, a utility shall file an annual report with the Commission, commencing with the calendar year 2023, that is due within 120 days of the end of the calendar year, and notifies the Commission of all security breaches within the calendar year affecting covered information maintained by a utility directly or through one of its contractors.

(4) For purposes of this section, a security breach means any unlawful or unauthorized acquisition, access, loss, theft, use or disclosure of customer data, including standard customer data or unshareable personal data.

ACCOUNTABILITY AND AUDITING

(q) Utilities shall be accountable for complying with the requirements herein, and must make available to the Commission upon request or audit:

(1) The notices that they provide to customers pursuant to these rules.

(2) Their internal and consumer-facing privacy and data security policies.

(3) The categories of agents, contractors and other third parties to which they disclose standard customer data for a primary purpose, the identities of agents, contractors and other third parties to which they disclose standard customer data for a secondary purpose, the purposes for which all such information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose. (Utilities shall retain and make available to the Commission upon request information concerning who has received standard customer data from them.)

(4) Copies of any secondary-use authorization forms by which the utility secures customer authorization for secondary uses of covered data.

(r) Customer Complaints. – Utilities shall provide customers with a process for

reasonable access to covered information, for correction of inaccurate covered information, and for addressing customer complaints regarding covered information under these rules.

(s) Training. – Utilities shall provide reasonable training to all employees and contractors who collect, use, store or process covered information.

(t) Audits. – Each utility shall conduct an independent audit, by an auditor selected or approved by the Commission, of its data privacy and security practices in conjunction with general rate case proceedings following 2023 and at other times as required by order of the Commission. The audit shall monitor compliance with data privacy and security commitments, and the utility shall report the findings to the Commission as part of the utility's general rate case filing.

(u) Reporting Requirements. – On an annual basis, each utility shall disclose to the Commission, as part of the annual report required by Rule R1-32, the following information:

(1) The number of authorized third parties accessing standard customer data.

(2) The number of non-compliances with this rule or with contractual provisions required by this rule experienced by the utility, and the number of customers affected by each non-compliance and a detailed description of each non-compliance.

Appendix B

Redline

~~Docket No. E-100, Sub 161~~
~~Attorney General's Office Proposed~~ Rule R8-51~~ and Initial Comments Appendix A~~

~~Rule R8-51~~. CUSTOMER AND THIRD-PARTY DATA ACCESS AND PRIVACY.

(a) Definitions.

(1) "Aggregated data" means usage data~~, alone~~ or ~~in combination with other~~ energy savings data~~,~~ at a premises from which ~~sufficient identifying information has been removed such that an~~no individual, family, household, residence~~,~~ or customer ~~cannot reasonably~~could be identified or ~~re-identified~~reidentified with reasonable effort in the judgment of the transferor if such data were made public. Before transferring any aggregated data, a transferor shall:

(i) Remove all information that could identify any particular individual, family, household, residence or customer;

(ii) Combine and/or process the data with the data of a sufficiently large group of customers in the manner described by this Rule; and

~~(i)~~(iii) In appropriate cases, utilize other anonymization techniques. Such techniques may include, without limitation, reducing the granularity of the data transferred or differential privacy.

(2) "Application programming interface" or "API" means a utility's internet-based system that securely provides customer data to customer-authorized third-parties using machine-to-machine communications.

(3) "Authorized third party" means a third party that has received authorization from a customer to access, receive, collect, store, use, or disclose standard customer data and that obtains the information from a utility.

(4) The "Commission" is the North Carolina Utilities Commission.

(5) "Covered information" means any information that is "standard customer data," "unshareable personal data," or "usage data" as defined in this rule. Covered information does not include, however, aggregated data. Covered information also does not include information provided to the Commission pursuant to its oversight responsibilities.

~~(6) The "primary purposes" for the collection, storage, use or disclosure of covered information are to:~~

(6) "Electric Services Purposes" means purposes relating to Commission-regulated electric power generation, transmission, distribution, delivery, and sales, and other regulated services, including, but not limited to, administration of customer accounts and rate schedules, metering, billing, standby service, backups, and changeovers of service to other suppliers.

~~(i) Provide or bill for electrical power;~~

Commented [A1]: The AGO and Public Staff's previous definitions focus only on data that are removed. But as the NIST has noted, merely removing identifying information is not enough because smart-meter data can be linked back to individuals with other datasets. For more information, see AGO Supplemental Comments filed July 22, 2022 (AGO Supplemental Comments), pages 7-8. This revised version also reflects the possibility of a centralized repository.

Commented [A2]: The utilities have complained that "primary purposes" was similar to "electric services" in their codes of conduct. We have replaced this definition with "Electric Services Purposes," which is based on the definition from their codes of conduct.

~~(ii) Provide for system, grid, or operational needs;~~

~~(iii) Provide services as required by state or federal law or as specifically authorized by an order of the Commission; or~~

~~(iv) Plan, implement, or evaluate demand response, energy management, or energy efficiency programs under contract with a utility, under contract with the Commission, or as part of a Commission authorized program conducted by a governmental entity under the supervision of the Commission.~~

(7) "Secondary purpose or use" means any purpose or use that is not ~~a primary~~an electric services purpose or use.

(8) "Standard customer data" means

(i) all energy usage data collected by a meter that a utility maintains as part of its regular records in the ordinary course of business, including kilowatt-hours used, load profile, and, where applicable to certain rate classes, kilo-volt-amps, kilo-volt-amperes-reactive, power factor, and the like;

(ii) customer-specific information including customer name, mailing address, premise address, any contact information, payment history, account number(s), and all information on bills including, but not limited to, line item charges and charge descriptions, amounts billed, the rate or tariff applicable to the account or meter, billing cycle dates, etc.; and

(iii) any information that might be necessary for participation in, or to determine customer eligibility for, bill payment assistance, renewable energy, demand-side management, load management, or energy efficiency programs**.**

Standard customer data does not include unshareable personal data.

(9) "Unshareable personal data" means the birth date, social security number, biometrics, bank and credit card account numbers, driver's license number, credit reporting information, bankruptcy or probate information, health information, or network or internet protocol address of the customer or any person at the customer's location. This personal information is specifically excluded from the definition of standard customer data and, as stated in subdivision (d)(9) of this Rule, will not be shared by a utility with any party other than the customer.

(10) "Usage data" is all energy usage data collected by a meter including but not limited to kilowatt-hours used, load profile, kilo-volt-amps, kilo-volt-amperes-reactive, power factor, kW, or voltage.

(11) For purposes of this rule, the word "utility" has the same meaning as is defined in Rule R8-2.

(12) For purposes of this rule, a "utility contractor" means any third party that provides services to a utility under contract with that utility.

TRANSPARENCY (NOTICE OF USE OF CUSTOMER INFORMATION)

(b) Notice.

(1) Generally. – Utilities shall protect covered information in their possession or control to maintain the privacy of customers. Utility contractors' permissible uses of data and obligations to protect data are governed by contract with the utility as set forth in subsection (d) of this rule.

(2) Notice Requirement. – Utilities shall provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the accessing, collection, storage, use, and intentional disclosure of covered information. Utilities shall also provide such notice regarding the compilation, use, and disclosure of aggregated data.

(3) When Provided. – Utilities shall provide a written notice that meets the requirements of subdivision (b)(2) when confirming a new customer account, and at least once a year, utilities shall inform customers how they may obtain an updated copy of this notice. Utilities shall provide a conspicuous link to such notices under subdivision (b)(2) on the home page of their websites. Moreover, utilities shall include a link to the notice in all electronic mail to customers. Utilities shall also provide this notice upon request by any party.

(4) Form. – The notice, which may take the form of or be included in a privacy policy, shall be labeled "Notice of How We Gather, Use and Disclose Your Information" and shall:

(i) Be written in easily understandable language; and

(ii) Be no longer than is necessary to convey the requisite information.

(5) Content. – The notice shall state clearly:

(i) The identity of the utility;

(ii) The effective date of the notice;

(iii) The utility's process for altering the notice, including how the customer will be informed of any alterations and where prior versions will be made available to customers; and

(iv) The title and contact information, including email address, postal address, web address, and telephone number, of an official at the utility who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or disclosure of covered information or aggregated data.

The notice shall also:

(v) Include a description of the standard customer data made available to customers;

(vi) Indicate the frequency with which standard customer data can be provided;

(vii) Explain that disclosure of customers' data to third parties affects customer privacy, providing insight into their energy-consuming behaviors and permitting inferences about customers' daily activities, absences from the home or business, patterns of behavior, and lifestyle;

(viii) Explain that customers, before they authorize the disclosure of their data to third parties, should consider how the third party would be able to access and use their data;

(ix) Explain that the privacy and security of customer account and usage data will be protected by the utility while the data is in the utility's possession or control, but that the utility is not responsible for the privacy or security of the data after it has been transferred successfully to the customer or to an authorized third party;

(x) Identify any charges that may be applicable for customers to access data that are not standard customer data;

(xi) State that standard customer data will not be disclosed to third parties without customers' express, written consent in a manner and form approved by the Commission;

(xii) Explain the utility's policies regarding the manner in which a customer can authorize access and disclosure of covered information to third parties;

(xiii) Describe how the customer can terminate authorized third-party access to covered information; ~~and~~

(xiv) Inform customers that, unless they opt out, covered information ~~may~~will be used to create aggregated data reports that will not contain customer-identifying information, ~~and~~ that the utility may provide such aggregated data to third parties, and that covered information may be shared confidentially with researchers subject to Commission Rule R8-51~~.~~;

(xv) Provide information about how a customer may opt out of the aforementioned use of their covered information; and

~~(xv)~~(xvi) Explain that unshareable personal information will not be shared by a utility with any party other than the customer at any time.

Commented [A3]: This proposal now contains an ability for customers to opt out.

(c) Purpose Specification. – The notice required under subsection (b) shall also provide:

(1) An explicit description of:

(i) Each category of covered information collected, used, stored or disclosed by the utility, and, for each category of covered information, the reasonably specific purposes for which it will be collected, stored, used, or disclosed.

(ii) Each category of covered information that is disclosed to third parties, and, for each such category:

(a) The purposes for which it is disclosed; and

(b) The categories of third parties to which it is disclosed.

(iii) The specific identities of those authorized third parties to whom data is disclosed for secondary purposes, and the secondary purposes for which the information is disclosed.

(2) The approximate period of time that covered information will be retained by the utility or utility contractor.

(3) A description of:

(i) The means by which customers may view, inquire about, or dispute their covered information; and

(ii) The means, if any, by which customers may limit the collection, use, storage or disclosure of covered information and the consequences to customers if they exercise such limits.

USE AND DISCLOSURE LIMITATION

(d) Use and Disclosure Limitations.

(1) Generally. – Utilities are authorized to use covered information to provide regulated utility service ~~in the ordinary course of business. Providing such service is a primary purpose~~for Electric Service Purposes.

(2) No Sale of Customer Information. – Utilities may not sell information about customers ~~or,~~ covered information, ~~other than~~or aggregated data~~, for consideration~~. However, utilities may require payment of ~~any kind~~approved charges and fees in the manner set forth by this Rule.

(3) Use of Covered Information by a Utility for ~~Primary~~Electric Service Purposes. – A utility may access, collect, store and use covered information without customer consent, provided the use is for ~~primary purposes~~Electric Service

Commented [A4]: Using revised definition.

Commented [A5]: Better reflecting the intent of the rule.

Purposes and no disclosure is made to a utility contractor except as allowed by subdivision (d)(4) below.

(4) Disclosure by a Utility Without Customer Consent. – A utility may disclose standard customer data to a utility contractor without customer consent only:

(i) When explicitly ordered to do so by the Commission; or

(ii) For a primary purpose being carried out under contract with and on behalf of the utility disclosing the data; provided that the utility shall, by contract, require the utility contractor to agree to use the data only for the primary purpose and to access, collect, store, use, and disclose the information pursuant to policies, practices and notification requirements no less protective than those under which the utility itself operates as required under this rule, unless otherwise directed by the Commission. As part of this contractual agreement, utilities shall require utility contractors to provide similar contractual protections for standard customer data in the context of all subsequent disclosures for ~~primary purposes~~Electric Service Purposes.

(5) Terminating Disclosures to Entities Failing to Comply With Their Privacy Assurances. – When a utility discloses standard customer data to a utility contractor under this subsection (d), it shall specify by contract, unless otherwise ordered by the Commission, that it shall be considered a material breach if the contractor engages in a pattern or practice of accessing, storing, using or disclosing the information in violation of the party's contractual obligations to handle the information pursuant to policies no less protective than those under which the utility from which the information was initially derived operates. If a utility determines in good faith that a utility contractor is in breach of its contract for this reason, the utility shall promptly cease disclosing the information to the contractor.

(6) Ban on Disclosure for Secondary Purposes Without Consent. – No utility shall use or disclose standard customer data to any party for any secondary purpose without obtaining the customer's prior, express, voluntary, authenticated authorization for each distinct secondary purpose. This authorization is not required when information is:

(i) Provided pursuant to a legal process;

(ii) Provided in situations of imminent threat to life or property; ~~or~~

(iii) Specifically authorized by the Commission pursuant to its jurisdiction and control; or

~~(iii)~~(iv) Otherwise expressly permitted by this Rule.

(7) Requirements for Authentications of Consent. – Customer authorizations to disclose customer data are authenticated, under this Rule, if the customer's identity is established in either oral, electronic or non-electronic form and can be documented by the utility. Separate authorization by each customer must be obtained for all secondary uses of covered information by a utility.

(8) Form of Consent. – The customer consent form or process must be approved by the Commission, and shall include:

(i) Information to adequately identify the customer, consistent with, and no more onerous than, a utility's authentication practices when a customer creates an online account on a utility's website or when a customer calls the utility by telephone;

(ii) The intended purpose and the use of the data being requested;

(iii) The time period (e.g., months, years) during which the secondary use will take place;

(iv) The category of information to be shared, with a succinct description of each; and

(v) ~~Commitment~~In the event a utility seeks to use customer data for a secondary purpose, a commitment to the customer that the utility shall be responsible for using the data only for the authorized secondary use and that the utility will continue to protect the privacy and security of the data in accordance with this rule.

If a consent is made by electronic means, the information provided shall be in spoken form, displayed on a screen, or otherwise displayed to the customer via the customer's preferred contact method. If a consent is made by oral means, the information listed in sub-subdivisions (i) through (iii) shall be obtained and provided in spoken form, but the commitment to the customer in sub-subdivision (iv) may be provided either in spoken form or by directing the customer to a website that provides the commitment to the customer.

(9) Ban on Disclosure of Unshareable Personal Data. – Nothing in this Rule shall allow, and utilities shall be prohibited from, providing unshareable personal data to any party other than the customer. However, network or internet protocol addresses may be shared by a utility to a utility contractor for ~~a primary~~an electric services purpose.

CUSTOMER ACCESS AND CONTROL

(Individual Participation)

(e) Customer Access and Control.

(1) Quality and Quantity of Standard Customer Data. – A utility shall maintain at least 24 months of standard customer data, or the period of time that a customer has had an account at a given address, whichever is less, in sufficient detail for a customer to understand his or her energy usage. The frequency interval of data must be commensurate with the capabilities of the meter or network technology used to serve the customer.

(2) Customer Access to Standard Customer Data. – As part of basic utility service, upon request, a utility shall provide a customer access to the customer's own standard customer data provided in electronic machine- readable format, in conformity with nationally recognized standards and best practices concerning form and frequency, such as the latest version of the North American Energy Standard Board's (NAESB) Req. 21, the Energy Services Provider Interface (ESPI), and in a manner that ensures adequate protections for the utility's system security and the continued privacy and security of the customer data during transmission.

(3) Cost. –When the data requested is standard customer data, is authorized by the customer, and the request pertains to a time period within the previous 24 months, the request for access will be fulfilled without charge. If requests are made for information other than standard customer data or data outside the 24 months preceding the request, and utilities seek to charge customers a fee to provide such data, the utility may charge an amount that the Commission deems reasonable based on the utility's marginal cost to provide those data.

(4) Control. – Customers have the right to share their own standard customer data with authorized third parties of their choice to obtain services or products provided by those third parties and to ensure accuracy of covered information held by utilities and utility contractors. Utilities shall provide customers with convenient mechanisms for:

(i) Granting and revoking authorization for secondary uses of standard customer data by third parties;

(ii) Disputing the accuracy or completeness of any covered information that a utility is storing or distributing for any primary or secondary purpose; and

(iii) Requesting corrections or amendments to any covered information that the utility is collecting, storing, using, or distributing for any primary or secondary purpose.

AUTHORIZED THIRD PARTY ACCESS TO

CUSTOMER DATA FROM A UTILITY

(f) Authorized Third Party Access to Standard Customer Data from a Utility.

(1) Third Party Access upon Customer Authorization. – For the period of time during which a customer has provided consent, utilities shall grant authorized third parties access to the customer's standard customer data in electronic machine-readable format, in conformity with nationally recognized standards and best practices concerning form and frequency, such as the latest version of the North American Energy Standards Board's (NAESB) Req. 21, the Energy Services Provider Interface (ESPI), and in a manner that ensures adequate protections for the utility's system security and the continued privacy of the data in transit from a utility to an authorized third party. Following receipt of a valid customer authorization as described below, utilities shall electronically initiate requested data to the third party within 90 seconds, unless the customer has requested data delivery by another method.

(2) Customer Authorization. – Utilities shall designate the categories of standard customer data available to authorized third parties in conformity with this rule and provide brief descriptions of those categories in plain language for customers to understand. For all methods of authorization described below, when a customer authorizes third party access, the customer will identify the categories of information the customer wishes to share. If an authorized third party specifies the data it would like permission to access, the utility shall display such request to customers using the aforementioned categorical designations. Separate authorization by each customer must be obtained for all disclosures of standard customer data except as otherwise provided for herein.

(3) Authorization Process. – A utility shall not disclose standard customer data to a third party unless an authorization is valid as described in this rule. A utility shall, regardless of the authorization method described in this Rule, use consistent customer information to validate the customer's identity in a manner that is no more onerous than a utility's authentication practices when a customer creates an online account on a utility's website or when a customer calls the utility by telephone. A utility shall provide the following methods for any customer to grant a valid authorization: non-electronic; customer-initiated electronic; and at least one authorized third-party initiated electronic method using an API that is non-proprietary to the utility and is commonly used in the industry by other utilities. In addition, a utility shall provide additional customer-requested authorized third-party initiated electronic methods described below subject to its capability to do so without substantial additional cost.

(i) Non-electronic methods. Any customer may submit an authorization to a utility by at least the following methods:

(a) By telephone, in which authorizations shall be processed, and data transmitted, within one (1) business day; or

(b) By mail to a utility's mailing address, in which case

authorizations shall be processed, and data transmitted, within one (1) business day.

(ii) Customer-initiated electronic methods. Any customer may submit an authorization to a utility by completing a web-based submission on a utility's website, consistent with nationally recognized standards and best practices. In this case, a utility shall allow direct online submission following completion without requiring email or an online account.

(iii) Customer-requested, authorized third party initiated electronic methods. A customer may interact directly with a third party and provide the third party with the customer's account number. The utility shall receive a customer's account number from the third party via API and seek authentication from the customer as well as customer consent via the customer's preferred contact method (such as by one-time passcode). Once authorized, the utility shall provide the requested data to the authorized third party via API. In this context, the utility will authenticate the customer's identity, process the request for access, and permit electronic authorization via API in a timeframe no longer than the time required for a customer to create an online account at a utility's website and access his or her standard customer data.

(4) Requirements of authorization. – For all authorization methods used, a utility shall

(i) Enable and require the designation of the authorized third party and the customer;

(ii) Enable and require the specification of the purpose for sharing the data and the intended use of the data by the authorized third party;

(iii) Enable and require the designation of the time period (e.g., months and years of both historic and future data) for which data is being requested. The utility shall provide customers the option to authorize an ongoing provision of data that is valid until revoked by the customer or provision for a specified period of time.

(iv) Enable and require the designation of the categories of standard customer data being requested in accordance with subdivision (f)(2).

(v) Provide notice to the customer that, following access or transfer, the utility shall not be responsible for monitoring or ensuring that the third party to whom the data is disclosed is maintaining the confidentiality of the data or using the data as intended by the customer.

(5) Revocation and Termination. – Customers have the right to revoke, at any time, any previously granted authorization. Termination of electric utility service also terminates consent to disclose customer data granted by the customer for the meter(s) or premise(s) where electric utility service has been terminated. A utility shall also permit an authorized third party to terminate its authorization, in which case a utility shall subsequently notify a customer of the termination via the customer's preferred contact method and confirm to the authorized third party that the termination is accepted.

(6) Opportunity to Revoke. – The consent of a residential customer shall continue without expiration if the customer has elected ongoing provision until revocation, but the utility must contact a customer once annually to inform the customer of the authorization(s) granted and to provide an opportunity for revocation. The utility shall use electronic means to make this annual notice if the utility holds electronic contact information for the customer. The consent of a non-residential customer shall continue in the same way, but a utility must notify a non-residential customer once, upon an initial authorization, to provide an opportunity for revocation.

(7) Modifications. – Changes of contact names for an organization, trade name, or utility over time do not invalidate consent as to the respective organization, trade name, or utility. Modifications to the consent form or process over time do not invalidate previous consent.

(8) Parity. – Utilities shall permit customers to revoke authorization for any secondary purpose of their standard customer data by the same mechanism(s) initially used to grant authorization.

(9) Eligibility Determinations. – To protect the privacy and security of covered information, utilities shall apply eligibility criteria as follows. To be eligible to receive standard customer data, authorized third parties shall be required by utilities to: (i) demonstrate technical capability to interact securely with the utility's servers; (ii) provide contact information and federal tax identification numbers to a utility; (iii) acknowledge receipt and review of these privacy and access Rules; (iv) not have been disqualified as an authorized third party provider in the past pursuant to processes outlined at subdivisions (h)(2)-(4); and (v) adopt and comply with the most updated version of the 2015 Department of Energy's Voluntary Code of Conduct Final Concepts and Principles for Data Privacy and the Smart Grid (the "DataGuard Seal") or a similar nationally accepted eligibility standard approved by the Commission as a necessary, comparable, reasonable and appropriate alternative.

(10) Descriptive rate schedules. – A utility shall include in its rate schedules a description of standard customer data that it is within the utility's technological and data capabilities to provide to the customer, to an authorized representative of the customer, or to an authorized third party recipient. At a minimum, the utility's rate schedule must provide the following:

(i) A description of standard customer data and the frequency of updates that will be available;

(ii) The method and frequency of standard customer data transmittal and access available (electronic, paper, etc.), pursuant to which data is provided to authorized third parties as soon as practicable following collection of the usage data, as well as the security protections or requirements for such transmittal;

(iii) A reasonable timeframe for processing requests, consistent with this rule; and

(iv) Any fees or charges associated with processing a request for usage data.

(11) Records of Disclosures. – The utility shall maintain records of all disclosures of covered information to third parties, including a copy of the customer's authorization to disclose standard customer data (unless it was in oral form) and a list of the information disclosed using the categories developed by the utility under subdivision (f)(2) of this Rule. The utility shall maintain records of standard customer data disclosures for a minimum of three years and shall make the records of the disclosure of a customer's data available for review by the customer upon request.

LIABILITY AND COMPLAINTS

(g) Liability. – Nothing in this Rule shall be construed to impose any liability on a utility or any of its directors, officers and employees, relating to disclosures of information when (1) the Commission orders the provision of standard customer data to a third party; or (2) a customer discloses covered data to, or authorizes access to standard customer data by, a third party that is unaffiliated with and has no other business relationship with the utility. Specifically, after a utility securely transfers covered information to a customer or standard customer data to an authorized third party pursuant to a customer's request, nothing in this Rule shall make a utility responsible for the security of the information or its use or misuse by such customer or by a third party. This section does not apply where a utility has acted recklessly.

(h) Complaints.

(1) Complaints Submitted by Customers Against Utilities. Complaints from customers regarding a utility's failure to process customer authorizations to release standard customer data pursuant to this Rule in a timely and accurate manner, or to provide eligible authorized third parties with access to a customer's standard customer data in a timely and accurate manner, or regarding the utility's failure to comply with this Rule in any other respect, shall be treated as complaints under Rule R1-9.

(2) Complaints Submitted to a Utility. If a utility disclosing standard customer data to a Commission-authorized or customer-authorized third party receives a customer complaint about the third party's misuse of data, the utility shall keep records of such complaints and submit a report to the Commission annually of any such complaints or suspected violations. If a utility believes it is necessary to terminate an authorized third party's access to customer data, the utility shall file a request with the Commission in accordance with subdivision (h)(3).

(3) Complaints submitted by a utility. If a utility has a reasonable suspicion that an authorized third party has engaged in conduct rendering it ineligible to access information under this Rule, the utility shall expeditiously inform the Commission and the Public Staff of any information regarding possible ineligibility.

(4) If the Commission confirms that a third party is or has become ineligible to receive information as an authorized third party under this Rule, the Commission shall allow the utility to refrain from providing or to discontinue providing standard customer data to that party.

A utility will not be deemed to have made a reckless transmission of covered information to an authorized third party if the utility acts consistently with the process described in subdivisions (2) and (3) above.

A utility is prohibited from unilaterally revoking access to an authorized third party for any reason other than a Commission order pursuant to paragraph 4 above or a good faith belief that the third party ~~is ineligible under this Rule or~~ poses an imminent danger to life, property or the cybersecurity of the utility's systems.

(i) Penalties. – An admission to or Commission adjudication of liability for a violation of these rules may result in an assessment of a civil penalty or fine as provided by 15 N.C. Gen. Stat. § 62-310 et seq.

AGGREGATED ~~USAGE~~ DATA

(j) Aggregated ~~Usage~~ Data.

(1) Availability of Aggregated ~~Usage~~ Data. – Utilities may permit the use of aggregated ~~usage~~ data from which all identifiable information has been removed to be used for analysis, reporting or program management provided that the release of that data does not disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information.

(2) Requests for Aggregated Data ~~Reports~~. Unless otherwise specified below, individual customers need not consent to requests for aggregated data in the following circumstances. If the requirements below are not met, then the

Commented [A6]: Using the defined term.

Commented [A7]: These are the main changes in the proposed rule.

requestors must secure and provide the utility evidence of explicit authorization from ~~a Utility. –~~each customer whose usage data are subject to the request.

(i) Publicly Available Aggregated Data. A utility ~~may disclose readily~~must make the following types of data available ~~aggregated data that consists of~~ on its public website:

(a) Usage data showing the total amount of energy used in one calendar year within the State of North Carolina, the utility, any municipality, any zip code, any census block group, or any census block. These data shall be posted as close to real-time as possible.

(b) Usage data showing the total amount of energy used in any quarter in the State of North Carolina, the utility, any municipality, any zip code, any census block group, or any census block. These data shall be updated at least ~~fifteen customers, where the data of a~~ once every six months.

(c) Usage data showing the total amount of energy used in any calendar month by the State of North Carolina, the utility, or a municipality. These data shall be updated at least once every six months.

(d) Usage data showing the total amount of energy used in any increment of time collected by the utility within the State of North Carolina. These data shall be updated at least once every six months.

(e) With respect to aggregated data for any municipality, the utility or the State of North Carolina, the utility shall provide such data with whether the usage is residential or nonresidential. These data shall be updated at least once every six months.

(ii) EnergyStar. If a requestor seeks aggregated data for a particular building or premises owned or operated by that requestor for the purposes of obtaining United States Environmental Protection Agency's EnergyStar certification or ranking, or complying with a law, ordinance or regulation related thereto, then a utility shall timely fulfill requests for aggregated data for that particular building or premises if the requirements below are met.

(a) *Only Monthly, Whole-Building Data in Usable Format.* The provided aggregated data shall consist only of monthly, whole-property consumption data for the requested building or premises. The utility shall provide updated data each month, if so requested, and in accordance with any best-practices document promulgated by the United States Environmental Protection Agency.

(b) *Residential or Commercial Units Only*: If the building or premises subject to the data request contains only residential units, commercial units, or a combination thereof, the

Commented [A8]: This follows the framework in Klaiber and Wilson's article.

Commented [A9]: We understand that it is difficult for owners and operators of buildings to obtain data for Energy Star certification. We utilize a 4/50 rule here based on PNNL research showing that reidentification becomes significantly harder after there are four customers in a building. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23786.pdf

requested usage data will be considered aggregated data if (1) all identifying information has been removed and (2) there are at least four customers, and no single ~~customer,~~customer's energy use equals or exceeds 50% of the total energy use in any given month.

(c) *Industrial Units*: If the building or premises ~~associated with a single~~contains any industrial units, the requestor must obtain the consent of the customers before obtaining aggregated data.

(d) If the aggregated data are being provided without customer~~, does not comprise 15 percent or more of the aggregated data.~~ consent, the recipient must enter into a nondisclosure agreement with the utility. That agreement must specify, at a minimum, that:

1. the requestor may use the aggregated data only for the purposes of building benchmarking, identifying energy efficiency projects, and energy management and complying with local laws and ordinances;
2. the requestor will not identify or reidentify any individual customers;
3. the requestor shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure; and
4. the requestor may not transfer the data to any other party, other than a third party who agrees not to transfer the data further and to abide by the other terms above.

(iii) Academic Researchers and Government Entities: Aggregated Data from Utility. – In ~~aggregating~~addition to the publicly available aggregated data above, academic researchers and government entities may obtain the aggregated data from a utility subject to the following terms:

(a) The following types of aggregated data will be made available:

1. Aggregated data showing the amount of energy used in one calendar month by any zip code, census block group, or census block per rate class.
2. Aggregated data showing the amount of energy used in one day by any municipality, zip code, census block group, or census block per rate class.
3. Aggregated data showing the amount of energy used in any increment of time longer than 15

Commented [A10]: From the Colorado PUC.

Commented [A11]: These are the other orange and yellow boxes from the Klass and Wilson article.

minutes by any municipality or zip code per rate class.

(b) An academic researcher or government entity shall execute a nondisclosure agreement in a form approved by the Commission. That nondisclosure agreement shall provide:

1. the recipient may use the usage data only for the purposes of studying energy;
2. the recipient party may not transfer any usage data to any other party;
3. the recipient will not identify or reidentify any individual customers; and
4. the recipient shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure, including that the usage data shall be destroyed after it has been used for the purposes of the program.

(iv) Public University Repository. – A public institution of higher education in North Carolina ("public university") may obtain two years' usage data together with the address of record and rate class with no other personally identifying information from a utility for no financial consideration. A public university receiving such usage data may obtain updated usage data every six months. A person who wishes to obtain aggregated data not otherwise available under this rule may request the data from the public university. The public university shall be required to execute a nondisclosure agreement with the utility in a form approved by the Commission. That nondisclosure agreement shall include at least the following terms:

(a) Implement commercially reasonable data security and cybersecurity measures including, but not limited to, physical and technical safeguards, limiting the number of people who may have access to such data to those with a need for such data, in addition to any safeguards that may be required by the institutional review board of the Public University.

(b) The public university may use the usage data only for academic, research or policy purposes. It may not use the usage data for purely commercial purposes.

(c) The public university may choose to provide aggregated data to third parties. That aggregated data must be either (1) otherwise available to the third party under this rule (e.g., publicly-available aggregated data) or (2) stripped of any personally-identifying information and anonymized using privacy-enhancing techniques, such as differential privacy, in a manner sufficient to prevent reidentification. The recipient must execute a nondisclosure agreement and agree to use the data only for energy-related purposes, not to transfer the

Commented [A12]: This allows public universities to act as repositories, as discussed in the AGO's current brief.

data to any other party, and not to attempt to reidentify any particular individual, family, household, residence or customer~~ data to create an aggregated data report, a utility must ensure the data does not include any~~ .

(d) The public university may not provide aggregated data to a third party if (1) the aggregated data reveal specific customer information because of the size of the group, rate classification, or nature of the information or (2) the aggregated data otherwise contain identifiable ~~customer~~critical infrastructure or other sensitive data~~. A utility~~ that should not be disclosed for security or, in the public university's view, extreme confidentiality purposes.

(e) In the event that the Public University or a party to whom the Public University provides any data publishes or otherwise provides information obtained from processing the data, any such publications or provisions shall not provide ~~aggregated~~enough information to permit reidentification of any individual, family, household, residence or customer ~~data in response to multiple overlapping requests from or on behalf of the same requestor that have the potential to identify~~ without extraordinary effort.

(f) The public university shall notify the Commission of any breach with respect to the usage data, and the Commission shall have audit rights over the public university's use of the data and may delegate those audit rights to other parties. The Commission may, in its discretion, cut off or reduce the public institution of higher education's access to the usage data if the Commission finds that it is not abiding by the terms of the nondisclosure agreement or this Rule.

(g) The public university shall be subject to reasonable data minimization and data retention policies.

(v) All requests for aggregated data shall be treated in accordance with the rate schedules to be filed pursuant to sub-subsection (j)(4). Such rate schedules may include additional categories of aggregated data not explicitly referenced in this rule. In the event no rate schedules that concern aggregated data have been filed, the utility shall nevertheless process requests for the categories of aggregated data explicitly mentioned in this rule as set forth herein.

~~(i)~~(vi) In the event that any provision concerning restrictions on the transfer of aggregated data without customer ~~data~~consent are deemed unlawful, this Rule shall be interpreted to provide the maximum protection against sharing or usage of the aggregated data without customer consent.

~~(2)~~(3) Opportunity to Revise Requests. – If an aggregated data report cannot be generated in compliance with this rule, the utility shall notify the requestor that the aggregated data, as requested, cannot be disclosed and identify the

reasons the request was denied. The requestor shall be given an opportunity to revise its aggregated data request in order to address the identified reasons.

~~(3)~~(4) Rate Schedules. – A utility shall file for Commission approval to amend its rate schedules to include a description of aggregated data reports available from the utility. At a minimum, the utility's rate schedules shall provide the following:

(i) A description of the aggregated data reports available from the utility, including all available selection parameters (usage data or other data);

(ii) The frequency of data collection;

(iii) The method of transmittal available (electronic, paper, etc.) and the security and privacy protections or requirements for such transmittal;

(iv) The applicable charges for providing an aggregated data report;

(v) The timeframe for processing requests; and

(vi) A form for requesting an aggregated data report to the utility identifying any information necessary from the requestor in order for the utility to process the request.

(5) Optouts. A customer may opt out of its data being provided to other parties under this subsection (j). In such a case, the utility shall not provide such customer's information to any other party.

(6) Any data a utility provides pursuant to this subsection (j) shall be provided in accordance with any best practice guidelines provided by the United States Environmental Protection Agency, with respect to EnergyStar-related data, as provided above, or the United States Department of Energy, with respect to any other data, within 90 days of the guidelines being promulgated.

REPORTING ON DISCLOSURES PURSUANT TO LEGAL PROCESS

(k) Disclosure Pursuant to Legal Process.

Except as otherwise provided in this rule, a court order, state or federal law, or by order of the Commission:

(1) Reporting. – On an annual basis, utilities shall report to the Commission the number of demands received for disclosure of customer data pursuant to legal process and the number of customers whose records were disclosed. Upon request of the Commission, utilities shall report additional information to the Commission on such disclosures. The Commission may make such reports publicly available without identifying the affected customers unless making

such reports public affects or would affect an ongoing criminal investigation.

DATA MINIMIZATION

(l) Data Minimization, Generally. – Utilities shall collect, store, use, and disclose only as much covered information as is reasonably necessary or as authorized by the Commission to accomplish the reasonably specific primary purpose identified in the notice required under subsections (b) and (c) or for a specific secondary purpose authorized by the customer.

(m) Data Retention. – Utilities shall maintain covered information only for as long as reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under subsections (b) and (c) or for a specific secondary purpose authorized by the customer.

(n) Data Disclosure. – Utilities shall not disclose to any third party more standard customer data than is reasonably necessary or as authorized by the Commission to carry out a specific primary purpose identified in the notice required under subsections (b) and (c) or for a specific secondary purpose authorized by the customer.

DATA QUALITY AND INTEGRITY

(o) Data Quality and Integrity. – Utilities shall ensure that covered information they collect, store, use, and disclose is reasonably accurate and complete or otherwise compliant with applicable rules and tariffs regarding the quality of energy usage data.

DATA SECURITY

(p) Data Security and Breach Notification.

(1) Generally. – Utilities shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

(2) Notification of Breach. – Notwithstanding and in addition to any other legal requirements, a utility shall require a utility contractor providing services to a utility for a primary purpose to notify the utility that is the source of the data within ~~one week~~24 hours (or, if in the utility's judgment a greater amount is necessary, 72 hours) of the detection of a security breach. Upon a security breach affecting 1,000 or more customers, whether by a utility or by a third party described herein, the utility shall notify the Commission of security breaches of covered information within two weeks of the detection of a security breach or within one week of notification by a third party of such a breach. Upon request by the Commission, utilities shall notify the Commission of security breaches of covered information.

(3) Annual Report of Breaches. – In addition, a utility shall file an annual report

with the Commission, commencing with the calendar year ~~2021~~2023, that is due within 120 days of the end of the calendar year, and notifies the Commission of all security breaches within the calendar year affecting covered information maintained by a utility directly or through one of its contractors.

(4) For purposes of this section, a security breach means any unlawful or unauthorized acquisition, access, loss, theft, use or disclosure of customer data, including standard customer data or unshareable personal data.

ACCOUNTABILITY AND AUDITING

(q) Utilities shall be accountable for complying with the requirements herein, and must make available to the Commission upon request or audit:

(1) The notices that they provide to customers pursuant to these rules.

(2) Their internal and consumer-facing privacy and data security policies.

(3) The categories of agents, contractors and other third parties to which they disclose standard customer data for a primary purpose, the identities of agents, contractors and other third parties to which they disclose standard customer data for a secondary purpose, the purposes for which all such information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose. (Utilities shall retain and make available to the Commission upon request information concerning who has received standard customer data from them.)

(4) Copies of any secondary-use authorization forms by which the utility secures customer authorization for secondary uses of covered data.

(r) Customer Complaints. – Utilities shall provide customers with a process for reasonable access to covered information, for correction of inaccurate covered information, and for addressing customer complaints regarding covered information under these rules.

(s) Training. – Utilities shall provide reasonable training to all employees and contractors who collect, use, store or process covered information.

(t) Audits. – Each utility shall conduct an independent audit, by an auditor selected or approved by the Commission, of its data privacy and security practices in conjunction with general rate case proceedings following ~~2020~~2023 and at other times as required by order of the Commission. The audit shall monitor compliance with data privacy and security commitments, and the utility shall report the findings to the Commission as part of the utility's general rate case filing.

(u) Reporting Requirements. – On an annual basis, each utility shall disclose to the Commission, as part of the annual report required by Rule R1-32, the following information:

(1) The number of authorized third parties accessing standard customer data.

(2) The number of non-compliances with this rule or with contractual provisions required by this rule experienced by the utility, and the number of customers affected by each non-compliance and a detailed description of each non-compliance.