

## Smart Grid Privacy Standards and Mitigating Controls

DRAFT 11.25.09

Rebecca Herold

1. **Limiting the collection** of data by the smart meter to only that necessary for the purposes of improving energy use and efficiency for the specific dwelling.
2. **Limiting the collection** of data by the utilities from the persons paying the utilities account at the dwelling to only that necessary to manage the account and to improve energy efficiency.
3. **Notify** the dwelling inhabitants (which may be different from the individuals paying the utilities bill for the dwelling) and persons paying the utilities bills of the data being collected, why it is necessary to collect the data, along with the specific uses for the data, the purpose for the collection, and the use, retention, and sharing of the data. Data subjects should be told this information before the time of collection.
4. **Notify** the dwelling inhabitants whenever the utility, or a smart grid entity, wants to start using existing collected data for different purposes.
5. **Notify** the dwelling inhabitants whenever the utility, or a smart grid entity, wants to start collecting additional data beyond that already being collected, along with provided a clear explanation for why the additional data is necessary.
6. Each utility and any other entity collecting energy usage data from or about dwellings must provide a clearly worded description to the dwelling inhabitants **notifying** them of 1) any **choices** available to individuals and, 2) explain why specified data items must be collected and used in specified ways without obtaining consent from the individual.
7. Each utility and any other entity collecting energy usage data from or about dwellings must describe the **choices** available to dwelling residents with regard to the use of their data and obtain explicit **consent** if possible, or implied consent when this is not feasible (such as for providing basic service), with respect to the collection, use and disclosure of the data collected from the specific dwelling.
8. Data, and subsequent created information that reveal personal information or activities, from and about specific dwellings should be **retained** only for as long as necessary to perform the purposes that have been communicated to the inhabitants. When no longer necessary the data and information, in all forms, should be irreversibly destroyed.
9. Data and created information from and about specific dwellings should only be **used or disclosed** for the specified purposes for which it was collected and should only be divulged to or **shared** with those parties authorized to receive it, and whom the organizations have told the dwelling inhabitants it would be shared.
10. Data and created information from and about specific dwellings should not be **disclosed** to or **shared** with any other parties except for those identified in the notices that have been provided to the dwelling inhabitants, or with the explicit **consent** of the individual.
11. Data collected from dwellings should be aggregated and anonymized by removing personally identifiable information elements wherever possible to ensure usage for data of individual dwellings are **limited** appropriately.
12. Each utility and any other entity collecting energy usage data from or about dwellings should provide a process to allow dwelling inhabitants to ask to see and be given **access to** the corresponding data from their specific dwelling, generated through their energy use and on their utilities account, and to request the correction of perceived inaccuracies.
13. Each utility and any other entity collecting energy usage data from or about dwellings must establish documented policies and procedures to ensure that the data collected from, and subsequently created about, dwelling inhabitants is **accurate, complete and relevant** for the purposes identified in the notice, and remains accurate throughout the life of the dwelling data within the control of the organization participating in the smart grid.
14. Each utility and any other entity collecting energy usage data from or about dwellings must make **privacy policies** available to dwelling inhabitants. Organizations participating in the smart grid must establish a procedure that allows dwelling inhabitants to verify the organization's compliance with their published privacy policies as well as their actual privacy practices.
15. Each utility and any other entity collecting energy usage data from or about dwellings must formally **assign responsibility** to a position or person to ensure that information security and privacy policies and practices exist and are followed. As part of their responsibilities, documented requirements for regular training and ongoing awareness activities must exist and be followed. Audit functions must also be present to monitor all data accesses and modifications.
16. Each utility and any other entity collecting energy usage data from or about dwellings must ensure that information in all forms, collected from, and subsequently created about, dwelling inhabitants, is

**appropriately protected** from loss, theft and must prevent unauthorized access, disclosure, copying, use or modification.

17. Each utility and any other entity collecting energy usage data from or about dwellings must **perform annual privacy impact assessments (PIAs)** and provide it to each state's energy commissioner office to review. They must also perform a PIA on each new system, network, or smart grid application and provide it to each state's energy commissioner office to review.
18. Each utility and any other entity collecting energy usage data from or about dwellings must establish policies and procedures to identify **breaches and misuse** of smart grid data, along with establishing procedures and plans for notifying dwelling inhabitants in a timely manner with appropriate details about the breach.
19. Each utility and any other entity collecting energy usage data from or about dwellings must **obtain and maintain a current organizational privacy certification** from an authorized third party certification organization to validate processes, policies and controls are in place that supports each of the previously listed applicable privacy standards. The organization should post an approved certification seal on their website to allow easy validation of their privacy certification.