We Claim:

1. A data monitoring system comprising:

a server communicatively coupled to a client device and a data module via a data network, wherein the server is configured to:

store a private key of a public-private key pair associated with the data module;

receive a request from the client device for authenticated access to the data module;

determine a first time by rounding a time maintained by the server to a time interval;

and

generate a first authentication key based at least on the private key and the first time, wherein the authentication key is used to allow authenticated access to the data module;

the client device configured to:

generate the request for authenticated access to the data module; and

transmit the request to the server; and

the data module including a user interface configured to display data and receive a user input, wherein the data module is configured to:

store the private key of the public-private key pair associated with the data module;

receive data from a medical device;

determine a second time by rounding a time maintained by the data module to the time interval such that the first time determined by the server and the second time determined by the data module are the same;

generate the authentication key based at least on the private key and the second time; and

in response to determining that the authentication key generated by the data module and the authentication key generated by the server match, grant authenticated access to the data module.

2. The system of claim 1, wherein the data module is further configured to, in response to determining that the second authentication key generated by the data module and the first authentication key generated by the server do not match, display a message indicating an authentication failure.

3. The system of claim 1, wherein the data module is configured to grant authenticated access using a challenge-response protocol.

4. The system of claim 1, wherein, upon successful authentication, the data module is configured to transmit the data to the client device.

5. The system of claim 1, wherein the time interval is adjustable to set a floor or ceiling of acceptable synchronization precision.

6. The system of any of claims 1-5, wherein the request for authenticated access to the data module includes additional information for instructing the data module.

7. The system of claim 6, wherein the additional information includes a request for access to the data module.

8. The system of any of claims 6-7, wherein the additional information includes a request for the data module to enter a maintenance mode.

9. The system of any of claims 1-7, wherein the authentication key is a one-time authentication key.

10. The system of claim 8, wherein the authentication key expires after a period of time.

11. The system of any of claims 1-9, wherein the private key is loaded into the data module during at least one of manufacturing or distribution of the data module.

12. The system of claim 10, wherein the private key is further stored by the server after the private key is loaded into the data module.

13. A method of securely monitoring a data module receiving data from a medical device, the method comprising:

storing, at a server, a private key of a public-private key pair associated with a data module;

receiving, at the server, a request from a client device for access to the data module;

determining, at the server, a first time by rounding a time maintained by the server to a time interval;

generating, at the server, a first authentication key based at least on the private key and the first time, wherein the first authentication key is used to allow authenticated access to the data module;

receiving, at the server, an indication from the data module that the first authentication key generated at the server was entered; and

in response to determining that the first authentication key generated by the server and a second authentication key generated by the data module match, granting the client device authenticated access to the data module wherein the second authentication key generated by the data module is generated based at least on the private key and a second time determined by the data module by rounding a time maintained by the data module to the time interval such that the first time determined by the server and the second time determined by the data module are the same.