

WHAT IS CLAIMED IS:

1. A data security system for enabling tokenized access to sensitive data, the data security system comprising a token provisioning computing device including a processor communicatively coupled to a memory device, the token provisioning computing device configured to:
 - 5 initiate a secure connection with a remote client computing device of a first data subject;
 - receive, from the remote client computing device of the first data subject, a request for an access token to provide a service provider computing device with access to sensitive data associated with the first data subject, wherein the request includes a data definition of the sensitive data to which access is to be provided and one or more authorization parameters including one or more data source identifiers of a respective one or more data sources at which the defined sensitive data is stored;
 - 10 generate the access token that enables access to the defined sensitive data from the one or more data sources according to the one or more authorization parameters;
 - store the access token in a token database with the data definition and the one or more authorization parameters; and
 - transmit, to the remote client computing device of the first data subject, a response including the access token and instructions that enable the remote computing device to at least one of display the access token to the first data subject and transmit the access token to the service provider computing device.
2. The data security system of Claim 1, wherein the token provisioning computing device is further configured to authenticate the request for the access token.
3. The data security system of Claim 2, wherein the request for the access token further includes authentication credentials input by the first data subject to the remote client computing device during a log-in process, and wherein to authenticate the request for the access token, the token provisioning computing device is further configured to process the authentication credentials received from the remote client computing device.

4. The data security system of Claim 2, wherein to authenticate the request for the access token, the token provisioning computing device is further configured to:

transmit an authentication request message to the remote client
5 computing device, the authentication request message including instructions that cause the remote client computing device to prompt the first data subject to input one or more authentication credentials into the remote client computing device;
receive, from the remote client computing device, an authentication
response message including the one or more input authentication credentials; and
10 process the input authentication credentials.

5. The data security system of Claim 1, wherein the token provisioning computing device is further configured to:

receive a token validation request message from the service provider
15 computing device, the token validation request message including the access token and a subject identifier associated with the data subject;
perform a lookup operation using at least one of the access token or the subject identifier;
when the lookup operation returns a valid and active stored access
20 token, validate the access token; and
transmit a token validation response message to the service provider
computing device, the token validation response message including an indication that the access token was successfully validated.

25 6. The data security system of Claim 1, wherein the token provisioning computing device is further configured to:

receive a token validation request message from a record integrator
associated with a healthcare provider (HCP) data manager that stores the sensitive
data to which access is to be provided and that is identified by the data source
30 authorization parameter, the token validation request message including the access token and a subject identifier associated with the data subject;
perform a lookup operation using at least one of the access token or the subject identifier;

when the lookup operation returns a valid and active stored access token, validate the access token; and

transmit a token validation response message to the record integrator, the token validation response message including an indication that the access token
5 was successfully validated.

7. The data security system of Claim 1, wherein the token provisioning computing device is further configured to:

receive a token validation request message from a healthcare provider
10 (HCP) data manager that stores the sensitive data to which access is to be provided and that is identified by the data source authorization parameter, the token validation request message including the access token and a subject identifier associated with the data subject;

perform a lookup operation using at least one of the access token or the
15 subject identifier;

when the lookup operation returns a valid and active stored access token, validate the access token; and

transmit a token validation response message to the HCP data manager, the token validation response message including an indication that the
20 access token was successfully validated.

8. The data security system of Claim 7, wherein the token validation response message further includes instructions that cause the HCP data manager to transmit the sensitive data to the service provider computing device.
25

9. The data security system of Claim 1, wherein the one or more authorization parameters further include at least one of a validity time/date parameter or an authorized service provider parameter.

30 10. The data security system of Claim 1, wherein the token provisioning computing device is further configured to:

receive, from the remote client computing device, data subject input indicating a revocation of the access token; and

in response to receiving the data subject input, at least one of delete the stored access token or disable the stored access token to prevent further access to the sensitive data by the service provider computing device.

5 11. The data security system of Claim 1, wherein the one or more authorization parameters include a validity date after which access to the sensitive data is revoked, and wherein the token provisioning computing device is further configured to:

 upon reaching the validity date, at least one of delete the stored access
10 token or disable the stored access token to prevent further access to the sensitive data by the service provider computing device.

 12. The data security system of Claim 1, wherein the access token is one of alphanumeric code, a bar code, and a QR code.

15

 13. A computer-implemented method for enabling tokenized access to sensitive data, the method implemented using a data security system including a token provisioning computing device including a processor communicatively coupled to a memory device, the method comprising:

20 initiating, by the token provisioning computing device, a secure connection with a remote client computing device of a first data subject;

 receiving, by the token provisioning computing device from the remote client computing device of the first data subject, a request for an access token to provide a service provider computing device with access to sensitive data associated
25 with the first data subject, wherein the request includes a data definition of the sensitive data to which access is to be provided and one or more authorization parameters including one or more data source identifiers of a respective one or more data sources at which the defined sensitive data is stored;

 generating, by the token provisioning computing device, the access
30 token that enables access to the defined sensitive data from the one or more data sources according to the one or more authorization parameters;

 storing, by the token provisioning computing device, the access token in a token database with the data definition and the one or more authorization parameters; and

transmitting, by the token provisioning computing device to the remote client computing device of the first data subject, a response including the access token and instructions that enable the remote computing device to at least one of display the access token to the first data subject and transmit the access token to the service provider computing device.

14. The method of Claim 13, wherein the request for the access token further includes authentication credentials input by the first data subject to the remote client computing device during a log-in process, the method further comprising authenticating the request for the access token by processing the authentication credentials received from the remote client computing device

15. The method of Claim 13, further comprising authenticating the request for the access token, the authenticating comprising:
transmitting an authentication request message to the remote client computing device, the authentication request message including instructions that cause the remote client computing device to prompt the first data subject to input one or more authentication credentials into the remote client computing device;
receiving, from the remote client computing device, an authentication response message including the one or more input authentication credentials; and
processing the input authentication credentials.

16. The method of Claim 13, further comprising:
receiving a token validation request message from the service provider computing device, the token validation request message including the access token and a subject identifier associated with the data subject;
performing a lookup operation using at least one of the access token or the subject identifier;
when the lookup operation returns a valid and active stored access token, validating the access token; and
transmitting a token validation response message to the service provider computing device, the token validation response message including an indication that the access token was successfully validated.

17. The method of Claim 13, further comprising:
receiving a token validation request message from a record integrator
associated with a healthcare provider (HCP) data manager that stores the sensitive
data to which access is to be provided and that is identified by the data source
5 authorization parameter, the token validation request message including the access
token and a subject identifier associated with the data subject;
performing a lookup operation using at least one of the access token or
the subject identifier;
when the lookup operation returns a valid and active stored access
10 token, validating the access token; and
transmitting a token validation response message to the record
integrator, the token validation response message including an indication that the
access token was successfully validated.

15 18. The method of Claim 13, further comprising:
receiving a token validation request message from a healthcare
provider (HCP) data manager that stores the sensitive data to which access is to be
provided and that is identified by the data source authorization parameter, the token
validation request message including the access token and a subject identifier
20 associated with the data subject;
performing a lookup operation using at least one of the access token or
the subject identifier;
when the lookup operation returns a valid and active stored access
token, validating the access token; and
25 transmitting a token validation response message to the HCP data
manager, the token validation response message including an indication that the
access token was successfully validated and instructions that cause the HCP data
manager to transmit the sensitive data to the service provider computing device

30 19. A non-transitory computer-readable storage medium having
computer-executable instructions stored thereon, wherein when executed by a
processor of a token provisioning computing device of a data security computing
system, the computer-executable instructions cause the processor to:

initiate a secure connection with a remote client computing device of a first data subject;

5 receive, from the remote client computing device of the first data subject, a request for an access token to provide a service provider computing device with access to sensitive data associated with the first data subject, wherein the request includes a data definition of the sensitive data to which access is to be provided and one or more authorization parameters including one or more data source identifiers of a respective one or more data sources at which the defined sensitive data is stored;

10 generate the access token that enables access to the defined sensitive data from the one or more data sources according to the one or more authorization parameters;

store the access token in a token database with the data definition and the one or more authorization parameters; and

15 transmit, to the remote client computing device of the first data subject, a response including the access token and instructions that enable the remote computing device to at least one of display the access token to the first data subject and transmit the access token to the service provider computing device.

20 20. The non-transitory computer-readable storage medium of Claim 19, wherein the access token is one of alphanumeric code, a bar code, and a QR code.