CLAIMS

1. A system comprising:

one or more processors; and

one or more memories storing instructions that, when executed by the one or more processors, cause the system to perform a process providing patient-specific healthcare data from an implant, the process comprising:

establishing a communicative contact with a patient-specific medical implant implanted in a body of a patient by a device associated with a user using a proximity communication mode,

wherein the patient-specific medical implant contains patient-specific healthcare data;

receiving, by the user, a request to access the patient-specific healthcare data in the patient-specific medical implant;

determining, based on an authentication level associated with the user, to provide the patient-specific healthcare data to the user and whether the patient-specific healthcare data is associated with the patient-specific medical implant;

in response to determining to provide the patient-specific healthcare data and the patient-specific healthcare data is associated with the patient-specific medical implant,

transmitting at least a portion of the patient-specific healthcare data for a physician managing treatment involving the patient-specific medical implant, wherein the patient-specific healthcare data includes one or more scans of the patient.

2. The system according to claim 1, wherein the process further comprises:

identifying one or more linked accounts from at least one entity related to the patient-specific healthcare data and the patient-specific medical implant;

determining whether the identified one or more linked accounts are authorized for receiving the patient-specific healthcare data; and

in response to determining that the one or more linked accounts are authorized, transmitting the patient-specific healthcare data to the at least one entity.

3. The system according to claim 1, wherein the process further comprises:

receiving the patient-specific healthcare data from at least one input data source;

storing the patient-specific healthcare data in a healthcare digital filing cabinet;

receiving data sharing rules from a patient owner of the healthcare digital filing cabinet; and

automatically transmitting the determined amount of the patient-specific healthcare data according to the received data sharing rules, wherein the data sharing rules include at least one of a physician sharing rule, a hospital sharing rule, or an implant manufacture sharing rule, wherein the data sharing rules include at least one a patient identifier setting, a data type sharing rule, or a meta data setting.

4. The system according to claim 1, wherein the process further comprises:

storing the patient-specific healthcare data in a healthcare digital filing cabinet;

linking accounts from multiple entities related to the patient-specific healthcare data into the healthcare digital filing cabinet.

5. The system according to claim 1, wherein the process further comprises:

encrypting the patient-specific healthcare data prior to transmission.

6. The system according to claim 1, wherein the process further comprises:

integrating input data sources of the patient-specific medical implant for the patient-specific healthcare data.

7. The system according to claim 1, wherein the patient-specific medical implant is a blockchain-enabled medical implant that is implanted in the body of a patient, wherein the process further comprises:

establishing the communicative contact using the proximity communication mode; and

accessing, based on the authentication level, a private key stored on the blockchain-enabled medical implant to access the patient-specific healthcare data in a healthcare digital filing cabinet.

8. The system according to claim 1, wherein the patient-specific healthcare data is locked such that the user cannot initially access the patient-specific healthcare data, wherein the process further comprises:

receiving authentication information from the user;

authenticating the user based on the received authentication information; and

in response to authenticating the user, unlocking a portion of the patient-specific healthcare data.

9. The system according to claim 1, wherein the process further comprises:

notifying the user of locking of a healthcare digital filing cabinet that contains the patient-specific healthcare data.

10. A non-transitory computer-readable medium storing instructions that, when executed by a computing system, cause the computing system to perform operations for providing patient-specific healthcare data from an implant, the operations comprising:

establishing a communicative contact with a patient-specific medical implant implanted in a body of a patient by a device associated with a user using a proximity communication mode,

wherein the patient-specific medical implant contains patient-specific healthcare data;

receiving, by the user, a request to access the patient-specific healthcare data in the patient-specific medical implant;

determining, based on an authentication level associated with the user, to provide the patient-specific healthcare data to provide to the user and whether the patient-specific healthcare data is associated with the patient-specific medical implant; and

in response to determining to provide the patient-specific healthcare data and the patient-specific healthcare data is associated with the patient-specific medical implant,

transmitting at least a portion of the patient-specific healthcare data for a physician managing treatment involving the patient-specific medical implant, wherein the patient-specific healthcare data includes one or more scans of the patient.

11. The non-transitory computer-readable medium of claim 10, wherein the operations further comprise:

identifying one or more linked accounts from at least one entity related to the patient-specific healthcare data and the patient-specific medical implant;

determining whether the identified one or more linked accounts are authorized for receiving the patient-specific healthcare data; and

in response to determining that the one or more linked accounts are authorized, transmitting the patient-specific healthcare data to the at least one entity.

12. The non-transitory computer-readable medium of claim 10, wherein the operations further comprise:

receiving the patient-specific healthcare data from at least one input data source;

storing the patient-specific healthcare data in a healthcare digital filing cabinet;

receiving data sharing rules from a patient owner of the healthcare digital filing cabinet; and

automatically transmitting the determined amount of the patient-specific healthcare data according to the received data sharing rules, wherein the data sharing rules include at least one of a physician sharing rule, a hospital sharing rule, or an implant manufacture sharing rule, wherein the data sharing rules include at least one a patient identifier setting, a data type sharing rule, or a meta data setting.

13. The non-transitory computer-readable medium of claim 10, wherein the operations further comprise:

storing the patient-specific healthcare data in a healthcare digital filing cabinet;

linking accounts from multiple entities related to the patient-specific healthcare data into the healthcare digital filing cabinet.

14. The non-transitory computer-readable medium of claim 10, wherein the operations further comprise:

encrypting the patient-specific healthcare data prior to transmission.

15. The non-transitory computer-readable medium of claim 10, wherein the operations further comprise:

integrating input data sources of the patient-specific medical implant for the patient-specific healthcare data.

16. The non-transitory computer-readable medium of claim 10, wherein the patient-specific medical implant is a blockchain-enabled medical implant that is implanted in the body of a patient, wherein the operations further comprise:

establishing the communicative contact using the proximity communication mode; and

accessing, based on the authentication level, a private key stored on the blockchain-enabled medical implant to access the patient-specific healthcare data in a healthcare digital filing cabinet.

17. The non-transitory computer-readable medium of claim 10, wherein the patient-specific healthcare data is locked such that the user cannot initially access the patient-specific healthcare data, wherein the operations further comprise:

receiving authentication information from the user;

authenticating the user based on the received authentication information; and

in response to authenticating the user, unlocking a portion of the patient-specific healthcare data.

18. The non-transitory computer-readable medium of claim 10, wherein the operations further comprise:

notifying the user of locking of a healthcare digital filing cabinet that contains the patient-specific healthcare data.

19. A computer-implemented method for providing patient-specific healthcare data from an implant, the method comprising:

establishing a communicative contact with a patient-specific medical implant implanted in a body of a patient by a device associated with a user using a proximity communication mode,

wherein the patient-specific medical implant contains patient-specific healthcare data;

receiving, by the user, a request to access the patient-specific healthcare data in the patient-specific medical implant;

determining, based on an authentication level associated with the user, to provide the patient-specific healthcare data to provide to the user and whether the patient-specific healthcare data is associated with the patient-specific medical implant; and

in response to determining to provide the patient-specific healthcare data and the patient-specific healthcare data is associated with the patient-specific medical implant,

transmitting at least a portion of the patient-specific healthcare data for a physician managing treatment involving the patient-specific medical implant, wherein the patient-specific healthcare data includes one or more scans of the patient.

20. The computer-implemented method of claim 19, further comprising:

identifying one or more linked accounts from at least one entity related to the patient-specific healthcare data and the patient-specific medical implant;

determining whether the identified one or more linked accounts are authorized for receiving the patient-specific healthcare data; and

in response to determining that the one or more linked accounts are authorized, transmitting the patient-specific healthcare data to the at least one entity.

21. The computer-implemented method of claim 19, further comprising:

receiving the patient-specific healthcare data from at least one input data source;

storing the patient-specific healthcare data in a healthcare digital filing cabinet;

receiving data sharing rules from a patient owner of the healthcare digital filing cabinet; and

automatically transmitting the determined amount of the patient-specific healthcare data according to the received data sharing rules.

22. The computer-implemented method of claim 21, wherein the data sharing rules include at least one of a physician sharing rule, a hospital sharing rule, or an implant manufacture sharing rule.

23. The computer-implemented method of claim 21, wherein the data sharing rules include at least one a patient identifier setting, a data type sharing rule, or a meta data setting.

24. The computer-implemented method of claim 19, wherein the patient-specific healthcare data includes one or more scans of the patient.

25. The computer-implemented method of claim 19, further comprising:

storing the patient-specific healthcare data in a healthcare digital filing cabinet;

linking accounts from multiple entities related to the patient-specific healthcare data into the healthcare digital filing cabinet.

26. The computer-implemented method of claim 19, further comprising:

encrypting the patient-specific healthcare data prior to transmission.

27. The computer-implemented method of claim 19, further comprising:

integrating input data sources of the patient-specific medical implant for the patient-specific healthcare data.

28. The computer-implemented method of claim 19, wherein the authentication level requires a two-factor authentication.

29. The computer-implemented method of claim 19, wherein the authentication level of the user is based on a geolocation, biometric data, or authentication credentials.

30. The computer-implemented method of claim 19, wherein the patient-specific medical implant is a blockchain-enabled medical implant that is implanted in the body of a patient, the method further comprising:

establishing the communicative contact using the proximity communication mode; and

accessing, based on the authentication level, a private key stored on the blockchain-enabled medical implant to access the patient-specific healthcare data in a healthcare digital filing cabinet.

31. The computer-implemented method of claim 19, wherein the user is a healthcare provider or a patient.

32. The computer-implemented method of claim 19, wherein the patient-specific healthcare data is locked such that the user cannot initially access the patient-specific healthcare data, the method further comprising:

receiving authentication information from the user;

authenticating the user based on the received authentication information; and

in response to authenticating the user, unlocking a portion of the patient-specific healthcare data.

33. The computer-implemented method of claim 32, wherein the authentication information indicates the authentication level.

34. The computer-implemented method of claim 19, further comprising:

receiving authentication information;

determining the authentication information is not valid; and

in response to determining the authentication information is not valid, locking a healthcare digital filing cabinet that contains the patient-specific healthcare data.

35. The computer-implemented method of claim 19, further comprising notifying the user of locking of a healthcare digital filing cabinet that contains the patient-specific healthcare data.

36. A computer-implemented method for providing patient-specific healthcare data associated with a patient-specific medical implant, the method comprising:

receiving the patient-specific healthcare data of a patient from at least one input data source;

generating, based on the patient-specific healthcare data, a patient-specific interactive surgical plan for implanting the patient-specific medical implant in a body of the patient;

receiving, from a user, a request to modify the patient-specific interactive surgical plan;

determining, based on an authentication level of the user, whether the user is authorized to modify the patient-specific interactive surgical plan;

in response to determining the user is authorized to modify the patient-specific interactive surgical plan, displaying, via a user-interface, the patient-specific interactive surgical plan;

detecting a modification to the patient-specific interactive surgical plan by the user;

modifying the patient-specific interactive surgical plan based on the modification of the patient-specific interactive surgical plan by the user, wherein a design and placement of the patient-specific medical implant is modified; and

storing the modified patient-specific interactive surgical plan in a healthcare digital filing cabinet.