BỘ Y TẾ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 3218 /QĐ-BYT	*Hà Nội, ngày 14 tháng 10 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy chế quản lý, vận hành, sử dụng, khai thác, chia sẻ dữ liệu và bảo đảm an ninh mạng Cổng dữ liệu sức khỏe của Bộ Y tế

BỘ TRƯỞNG BỘ Y TẾ

Căn cứ Luật Khám bệnh, chữa bệnh số 15/2023/QH15;

Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;

Căn cứ Luật Dữ liệu số 60/2024/QH15;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;

Căn cứ Luật Phòng bệnh số 114/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Căn cứ Luật Chuyển đổi số số 148/2025/QH15;

Căn cứ Nghị định số 102/2025/NĐ-CP ngày 13 tháng 5 năm 2025 của Chính phủ quy định quản lý dữ liệu y tế;

Căn cứ Nghị định số 165/2025/NĐ-CP ngày 30 tháng 6 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu;

Căn cứ Nghị định số 194/2025/NĐ-CP ngày 03 tháng 7 năm 2025 của Chính phủ quy định chi tiết một số điều của luật giao dịch điện tử về cơ sở dữ liệu quốc gia, kết nối và chia sẻ dữ liệu, dữ liệu mở phục vụ giao dịch điện tử của cơ quan nhà nước;

Căn cứ Nghị định số 278/2025/NĐ-CP ngày 22 tháng 10 năm 2025 của Chính phủ quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ về quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 224/2026/NĐ-CP ngày 24 tháng 6 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Chuyển đổi số;

Căn cứ Nghị định số 313/2026/NĐ-CP ngày 08 tháng 8 năm 2026 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Y tế;

Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;

Căn cứ Nghị định số 333/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng;

Căn cứ Quyết định số 20/2025/QĐ-TTg ngày 01 tháng 7 năm 2025 của Thủ tướng Chính phủ về việc Ban hành danh mục dữ liệu quan trọng, dữ liệu cốt lõi;

Căn cứ Quyết định số 1272/QĐ-BYT ngày 6 tháng 5 năm 2026 của Bộ trưởng Bộ Y tế phê duyệt Kế hoạch triển khai nhiệm vụ khám sức khỏe định kỳ hoặc khám sàng lọc miễn phí ít nhất mỗi năm một lần cho người dân;

Căn cứ Quyết định số 1551/QĐ-BYT ngày 31 tháng 5 năm 2026 của Bộ trưởng Bộ Y tế ban hành Hướng dẫn thu thập, cập nhật, kết nối liên thông dữ liệu khám sức khỏe và tạo lập, cập nhật Sổ sức khỏe điện tử trên ứng dụng VNeID;

Căn cứ Quyết định số 2062/QĐ-BYT ngày 8 tháng 7 năm 2026 sửa đổi một số nội dung của Quyết định số 1551/QĐ-BYT ngày 31 tháng 5 năm 2026 của Bộ trưởng Bộ Y tế ban hành Hướng dẫn thu thập, cập nhật, kết nối liên thông dữ liệu khám sức khỏe và tạo lập, cập nhật Sổ sức khỏe điện tử trên ứng dụng VNeID,

Theo đề nghị của Giám đốc Trung tâm Thông tin y tế Quốc gia và Cục trưởng Cục Quản lý Khám, chữa bệnh.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành, sử dụng, khai thác, chia sẻ dữ liệu và bảo đảm an ninh mạng Cổng dữ liệu sức khỏe của Bộ Y tế.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký, ban hành.

Điều 3. Các Ông/Bà: Chánh Văn phòng Bộ, Cục trưởng Cục Quản lý Khám, chữa bệnh, Giám đốc Trung tâm Thông tin y tế Quốc gia; Thủ trưởng các đơn vị thuộc và trực thuộc Bộ Y tế, Giám đốc Sở Y tế các tỉnh, thành phố trực thuộc Trung ương và Thủ trưởng các cơ quan, đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng (để báo cáo);
- Các đồng chí Thứ trưởng;
- Các Bộ, Cơ quan ngang Bộ, Cơ quan thuộc Chính phủ;
- UBND các tỉnh/thành phố;
- Các Bệnh viện trực thuộc Bộ Y tế;
- Y tế bộ, ngành;
- SYT các tỉnh, thành phố;
- Lưu: VT, KCB, TTYQG.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG THƯỜNG TRỰC

Vũ Mạnh Hà

BỘ Y TẾ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ

Quản lý, vận hành, sử dụng, khai thác, chia sẻ dữ liệu và bảo đảm an ninh mạng Cổng dữ liệu sức khoẻ của Bộ Y tế

(Ban hành kèm theo Quyết định số 3218/QĐ-BYT ngày 14 tháng 10 năm 2026 của Bộ trưởng Bộ Y tế)

Chương I. QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định nguyên tắc, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc quản lý, vận hành, sử dụng, khai thác, xử lý, kết nối, chia sẻ dữ liệu và bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân đối với Cổng dữ liệu sức khỏe của Bộ Y tế.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với các đơn vị thuộc, trực thuộc Bộ Y tế; Sở Y tế các tỉnh, thành phố trực thuộc Trung ương; các cơ sở khám bệnh, chữa bệnh; các cơ quan, tổ chức, đơn vị và cá nhân khác có liên quan đến việc quản lý, vận hành, sử dụng, khai thác, xử lý, kết nối, chia sẻ dữ liệu và bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân đối với Cổng dữ liệu sức khỏe của Bộ Y tế.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *Cổng dữ liệu sức khỏe của Bộ Y tế* (sau đây gọi tắt là Hệ thống) là hệ thống thông tin do Bộ Y tế xây dựng, quản lý nhằm thu thập, tiếp nhận, lưu trữ, cập nhật, đồng bộ, khai thác và chia sẻ dữ liệu sức khỏe của người dân; phục vụ việc tạo lập, cập nhật dữ liệu khám sức khỏe định kỳ hoặc khám sàng lọc, dữ liệu khám bệnh và các dữ liệu sức khỏe khác theo quy định của pháp luật; phục vụ tạo lập, cập nhật Sổ sức khỏe điện tử trên ứng dụng VNeID; đồng thời thực hiện kết nối, liên thông, chia sẻ dữ liệu với các cơ sở dữ liệu và hệ thống thông tin có liên quan.

Hệ thống bao gồm các thành phần chính sau đây:

a) Cơ sở dữ liệu sức khỏe cá nhân;

b) Phần mềm bao gồm các chức năng: cập nhật dữ liệu, tiếp nhận dữ liệu, quản lý dữ liệu, theo dõi tiếp nhận dữ liệu, báo cáo, thống kê và Bảng thông tin tổng hợp (Dashboard);

c) Giao diện lập trình ứng dụng (API) phục vụ kết nối, liên thông, đồng bộ, chia sẻ dữ liệu giữa Bộ Y tế với các cơ quan, tổ chức, đơn vị theo quy định của pháp luật.

2. *Cơ sở dữ liệu sức khỏe cá nhân* bao gồm: Dữ liệu khám sức khỏe định kỳ, khám sàng lọc của người dân được thu thập từ các cơ sở khám bệnh, chữa bệnh và dữ liệu khám bệnh của người dân được chia sẻ, đồng bộ từ Bảo hiểm xã hội Việt Nam và các dữ liệu sức khỏe khác theo quy định của pháp luật và Bộ Y tế.

3. *Sổ sức khỏe điện tử trên ứng dụng VNeID* giúp người dân tra cứu thông tin về sức khỏe của mình và thực hiện các thủ tục hành chính. Nội dung, phạm vi thông tin được tích hợp, chia sẻ và hiển thị trên Sổ sức khỏe điện tử trên ứng dụng VNeID thực hiện theo quy định của Bộ Y tế và cơ quan có thẩm quyền.

4. *Tài khoản liên thông:* là tài khoản hoặc thông tin xác thực được cấp cho cơ quan, tổ chức để thực hiện kết nối, đồng bộ, trao đổi, chia sẻ dữ liệu với Hệ thống.

5. *Tài khoản sử dụng*: là tài khoản được cấp cho cơ quan, tổ chức hoặc cá nhân để truy cập, sử dụng các chức năng của Hệ thống theo phạm vi được phân quyền.

6. *Giao diện lập trình ứng dụng (Application Programming Interface - API)* là tập hợp các quy tắc, giao thức và phương thức cho phép các hệ thống thông tin, phần mềm hoặc cơ sở dữ liệu kết nối, trao đổi và chia sẻ dữ liệu với nhau.

7. *Tiếp nhận dữ liệu*: là quá trình Hệ thống nhận dữ liệu từ các hệ thống thông tin, cơ sở dữ liệu hoặc từ người sử dụng để lưu trữ, xử lý, khai thác theo quy định.

8. *Bảng thông tin tổng hợp (Dashboard)*: là giao diện hiển thị các chỉ tiêu, báo cáo, biểu đồ phục vụ theo dõi, quản lý, điều hành và hỗ trợ ra quyết định.

9. *Đơn vị quản lý hệ thống:* là Trung tâm Thông tin y tế Quốc gia thuộc Bộ Y tế.

10. *Đơn vị vận hành hệ thống:* là cơ quan, tổ chức, đơn vị được giao nhiệm vụ hoặc được thuê thực hiện các hoạt động vận hành kỹ thuật, giám sát, bảo trì, hỗ trợ người sử dụng và bảo đảm Hệ thống hoạt động ổn định, liên tục, an toàn.

11. *Quản trị hệ thống:* là cá nhân được phân công thực hiện các nhiệm vụ cấu hình, quản lý người dùng, phân quyền, giám sát hoạt động và bảo đảm an ninh hệ thống thông tin của Hệ thống.

12. *Quản trị cơ sở dữ liệu:* là cá nhân được phân công quản lý, vận hành, sao lưu, khôi phục, tối ưu và bảo đảm tính toàn vẹn, tính sẵn sàng của cơ sở dữ liệu thuộc Hệ thống.

Điều 4. Nguyên tắc chung quản lý, vận hành, sử dụng, khai thác, chia sẻ dữ liệu và bảo đảm an ninh mạng

1. Việc quản lý, vận hành, sử dụng, khai thác, xử lý, kết nối, chia sẻ dữ liệu và bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân đối với Hệ thống phải tuân thủ quy định của pháp luật về dữ liệu, bảo vệ dữ liệu cá nhân, khám bệnh, chữa bệnh, giao dịch điện tử, an ninh mạng, bảo vệ bí mật nhà nước và các quy định pháp luật có liên quan.

2. Việc thu thập, tạo lập, cập nhật, lưu trữ, xử lý, khai thác, sử dụng dữ liệu sức khỏe trên Hệ thống phải bảo đảm:

a) Đúng mục đích, đúng đối tượng, đúng thẩm quyền, đúng phạm vi và có căn cứ theo quy định của pháp luật;

b) Tuân thủ nguyên tắc tối thiểu hóa dữ liệu, chỉ xử lý dữ liệu trong phạm vi cần thiết để thực hiện chức năng, nhiệm vụ, quyền hạn được giao;

c) Bảo đảm tính chính xác, đầy đủ, kịp thời, thống nhất và toàn vẹn của dữ liệu;

d) Bảo đảm quyền và lợi ích hợp pháp của chủ thể dữ liệu theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

3. Cơ quan, tổ chức, đơn vị tạo lập, cập nhật hoặc cung cấp dữ liệu lên Hệ thống chịu trách nhiệm về tính chính xác, đầy đủ, kịp thời, hợp pháp và chất lượng của dữ liệu; bảo đảm dữ liệu "đúng, đủ, sạch, sống" theo hướng dẫn của Bộ Y tế.

4. Việc kết nối, chia sẻ dữ liệu phải bảo đảm đúng mục đích, đúng đối tượng, đúng phạm vi, đúng thẩm quyền; tuân thủ quy định về kiến trúc dữ liệu, quản trị dữ liệu, tiêu chuẩn, quy chuẩn kỹ thuật, chuẩn dữ liệu và các yêu cầu về an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

5. Công tác bảo đảm an ninh mạng, an ninh dữ liệu phải được thực hiện thường xuyên, liên tục, chủ động phòng ngừa, phát hiện, cảnh báo, ngăn chặn, ứng cứu, khắc phục và xử lý kịp thời các nguy cơ, sự cố theo quy định của pháp luật.

6. Các hành vi không được thực hiện

a) Cản trở trái pháp luật việc kết nối, khai thác, sử dụng dữ liệu hợp pháp của cơ quan, tổ chức, cá nhân;

b) Thu thập, truy cập, khai thác, sử dụng, sao chép, trích xuất, cung cấp, chia sẻ, chuyển giao hoặc tiết lộ dữ liệu trái quy định của pháp luật hoặc vượt quá phạm vi được giao;

c) Sử dụng dữ liệu không đúng mục đích hoặc xâm phạm quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

d) Làm sai lệch, giả mạo, hủy hoại, xóa hoặc thay đổi trái phép dữ liệu;

đ) Mua bán, trao đổi trái phép dữ liệu;

e) Xâm nhập trái phép, phá hoại hạ tầng kỹ thuật hoặc thực hiện hành vi làm gián đoạn, cản trở hoạt động của Hệ thống;

g) Các hành vi khác bị nghiêm cấm theo quy định của pháp luật.

7. Dữ liệu sức khỏe thuộc danh mục dữ liệu quan trọng, dữ liệu cốt lõi được quản lý, bảo vệ theo quy định của pháp luật.

CHƯƠNG II. QUẢN LÝ, VẬN HÀNH VÀ SỬ DỤNG CỔNG DỮ LIỆU SỨC KHỎE CỦA BỘ Y TẾ

Điều 5. Quản lý, vận hành hệ thống

1. Trung tâm Thông tin y tế Quốc gia là đơn vị quản lý Hệ thống, chịu trách nhiệm tổ chức quản lý, điều phối, kiểm tra, giám sát hoạt động vận hành Hệ thống theo quy định của pháp luật và Quy chế này.

2. Đơn vị quản lý Hệ thống có trách nhiệm

a) Tổ chức quản lý, điều phối và giám sát hoạt động vận hành Hệ thống, bảo đảm Hệ thống hoạt động ổn định, liên tục, an toàn;

b) Tổ chức tiếp nhận, quản lý, lưu trữ, đồng bộ, kết nối, chia sẻ và khai thác dữ liệu theo quy định của pháp luật và Quy chế này;

c) Theo dõi, giám sát hoạt động của Hệ thống; kịp thời phát hiện, xử lý hoặc phối hợp xử lý sự cố, bảo đảm Hệ thống hoạt động an toàn, liên tục;

d) Ban hành hoặc trình cấp có thẩm quyền ban hành các quy trình, hướng dẫn kỹ thuật phục vụ quản lý, vận hành Hệ thống;

đ) Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tổ chức hướng dẫn, hỗ trợ, kiểm tra việc sử dụng Hệ thống.

3. Đơn vị vận hành Hệ thống là đơn vị được giao nhiệm vụ hoặc được thuê thực hiện vận hành kỹ thuật Hệ thống; chịu sự quản lý, điều phối, kiểm tra, giám sát của đơn vị quản lý Hệ thống và chịu trách nhiệm về chất lượng vận hành trong phạm vi nhiệm vụ được giao.

4. Các cơ quan, tổ chức, đơn vị và cá nhân có liên quan có trách nhiệm phối hợp với đơn vị quản lý Hệ thống và đơn vị vận hành Hệ thống trong quá trình quản lý, vận hành, xử lý sự cố và thực hiện các nhiệm vụ có liên quan theo quy định.

Điều 6. Quản lý hạ tầng kỹ thuật

1. Hạ tầng kỹ thuật của Hệ thống phải được quản lý, vận hành bảo đảm hiệu năng, tính sẵn sàng, khả năng mở rộng, khả năng dự phòng, tính liên tục của dịch vụ và đáp ứng yêu cầu về an ninh mạng theo quy định của pháp luật.

2. Đơn vị quản lý Hệ thống có trách nhiệm tổ chức quản lý, kiểm tra, giám sát việc vận hành hạ tầng kỹ thuật; xác định yêu cầu về năng lực, hiệu năng, dự

phòng và tính sẵn sàng; chỉ đạo, điều phối việc xử lý các sự cố, nguy cơ ảnh hưởng đến hoạt động của Hệ thống.

3. Việc bảo trì, nâng cấp, thay đổi hoặc mở rộng hạ tầng kỹ thuật phải được lập kế hoạch, đánh giá ảnh hưởng, tổ chức thực hiện theo quy trình quản lý vận hành và quản lý thay đổi của Hệ thống. Trường hợp có khả năng ảnh hưởng đến hoạt động của Hệ thống thì phải thông báo trước cho các cơ quan, tổ chức, đơn vị sử dụng, trừ trường hợp khẩn cấp hoặc để xử lý sự cố.

4. Việc quản lý, vận hành hạ tầng kỹ thuật phải tuân thủ các quy định của pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật và yêu cầu của Hệ thống về an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân, sao lưu, dự phòng và phục hồi hoạt động.

5. Đơn vị vận hành Hệ thống có trách nhiệm thực hiện vận hành kỹ thuật hạ tầng theo phạm vi được giao; theo dõi, giám sát tài nguyên, hiệu năng, tình trạng hoạt động; thực hiện bảo trì, xử lý sự cố, khắc phục lỗi kỹ thuật và báo cáo kịp thời cho đơn vị quản lý Hệ thống về các nguy cơ, sự cố hoặc tình trạng có thể ảnh hưởng đến hoạt động của Hệ thống.

Điều 7. Quản lý phần mềm ứng dụng

1. Phần mềm ứng dụng của Hệ thống phải được quản lý thống nhất, bảo đảm hoạt động ổn định, liên tục, an toàn, đáp ứng yêu cầu quản lý, vận hành, khai thác, kết nối, chia sẻ dữ liệu và phát triển Hệ thống.

2. Việc phát triển, nâng cấp, chỉnh sửa hoặc thay đổi phần mềm phải được thực hiện theo quy trình quản lý thay đổi của Hệ thống; được đánh giá về phạm vi ảnh hưởng, tính tương thích, an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân và khả năng duy trì hoạt động liên tục của Hệ thống trước khi triển khai.

3. Trước khi đưa phiên bản phần mềm mới hoặc nội dung nâng cấp vào vận hành chính thức, phải thực hiện kiểm tra, thử nghiệm, đánh giá, nghiệm thu theo quy định; bảo đảm đáp ứng yêu cầu nghiệp vụ, kỹ thuật, an ninh mạng, an ninh dữ liệu và bảo vệ dữ liệu cá nhân. Trường hợp việc triển khai có ảnh hưởng đến hoạt động hoặc cách thức sử dụng Hệ thống thì phải thông báo, hướng dẫn cơ quan, tổ chức, đơn vị sử dụng trước khi triển khai, trừ trường hợp khẩn cấp.

4. Đơn vị quản lý Hệ thống có trách nhiệm quản lý phiên bản phần mềm, phê duyệt hoặc tổ chức phê duyệt thay đổi theo thẩm quyền, lưu trữ hồ sơ thay đổi và giám sát quá trình triển khai các phiên bản phần mềm trên Hệ thống.

5. Đơn vị vận hành Hệ thống có trách nhiệm triển khai kỹ thuật các phiên bản phần mềm theo kế hoạch và yêu cầu của đơn vị quản lý Hệ thống; thực hiện phương án sao lưu, khôi phục khi cần thiết; theo dõi hoạt động của Hệ thống sau triển khai; kịp thời phát hiện, xử lý hoặc phối hợp xử lý lỗi, sự cố phát sinh và báo cáo đơn vị quản lý Hệ thống.

Điều 8. Sao lưu, phục hồi dữ liệu

1. Dữ liệu trên Hệ thống phải được sao lưu, lưu trữ và bảo đảm khả năng phục hồi nhằm duy trì tính toàn vẹn, tính sẵn sàng và tính liên tục của Hệ thống.

2. Đơn vị quản lý Hệ thống có trách nhiệm xây dựng hoặc tổ chức xây dựng, phê duyệt theo thẩm quyền và định kỳ rà soát, cập nhật phương án sao lưu, lưu trữ, phục hồi dữ liệu; xác định yêu cầu về phạm vi, tần suất sao lưu, thời gian lưu giữ, khả năng phục hồi và các yêu cầu bảo vệ dữ liệu.

3. Việc sao lưu, lưu trữ và phục hồi dữ liệu phải tuân thủ quy định của pháp luật về dữ liệu, bảo vệ dữ liệu cá nhân, an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước và các quy định pháp luật có liên quan.

4. Đơn vị quản lý Hệ thống tổ chức kiểm tra, đánh giá định kỳ hoặc đột xuất khả năng sao lưu, phục hồi dữ liệu; yêu cầu khắc phục kịp thời các tồn tại, hạn chế nhằm bảo đảm khả năng phục hồi và hoạt động liên tục của Hệ thống khi xảy ra sự cố.

5. Đơn vị vận hành Hệ thống có trách nhiệm thực hiện sao lưu, lưu trữ, phục hồi dữ liệu theo phương án và phạm vi nhiệm vụ được giao; theo dõi kết quả sao lưu, kiểm tra tính khả dụng của bản sao lưu, kịp thời xử lý hoặc báo cáo đơn vị quản lý Hệ thống khi phát hiện lỗi, mất dữ liệu hoặc nguy cơ ảnh hưởng đến khả năng phục hồi của Hệ thống.

Điều 9. Quản lý tài khoản và phân quyền

1. Việc quản lý tài khoản và phân quyền truy cập Hệ thống phải bảo đảm đúng đối tượng, đúng thẩm quyền, phù hợp với chức năng, nhiệm vụ, phạm vi quản lý và yêu cầu bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân.

2. Tài khoản sử dụng Hệ thống phải được gắn với cơ quan, tổ chức hoặc cá nhân được cấp; không được sử dụng chung, cho mượn, chuyển nhượng hoặc sử dụng trái mục đích, trái phạm vi được phân quyền.

3. Đơn vị quản lý Hệ thống, Sở Y tế hoặc cơ sở khám, chữa bệnh theo phân cấp phạm vi quản lý có trách nhiệm cấp, thay đổi, tạm khóa, mở khóa, thu hồi tài khoản và phân quyền truy cập theo đề nghị của cơ quan, tổ chức có thẩm quyền hoặc theo quy định của Quy chế này.

4. Thủ trưởng cơ quan, tổ chức, đơn vị được cấp quyền quản lý tài khoản có trách nhiệm quản lý việc sử dụng tài khoản thuộc phạm vi quản lý; kịp thời đề nghị điều chỉnh, tạm khóa hoặc thu hồi tài khoản khi có thay đổi về nhân sự, chức năng, nhiệm vụ hoặc khi phát hiện nguy cơ mất an toàn, an ninh.

5. Người sử dụng tài khoản có trách nhiệm quản lý, sử dụng tài khoản đúng mục đích, đúng phạm vi được phân quyền; bảo mật thông tin xác thực; tuân thủ các yêu cầu bảo vệ tài khoản; kịp thời thông báo khi phát hiện tài khoản có dấu hiệu bị lộ, bị chiếm quyền sử dụng hoặc bị sử dụng trái phép.

6. Việc phân quyền truy cập phải tuân thủ nguyên tắc quyền tối thiểu, phù hợp với chức năng, nhiệm vụ, phạm vi quản lý và nhu cầu khai thác dữ liệu; quyền truy cập phải được rà soát định kỳ và khi có thay đổi liên quan.

7. Đơn vị quản lý Hệ thống có trách nhiệm quản lý tài khoản quản trị Hệ thống, tài khoản quản trị cơ sở dữ liệu và các tài khoản có quyền truy cập đặc biệt; ban hành hoặc tổ chức thực hiện quy trình quản lý tài khoản, phân quyền, xác thực và thu hồi quyền truy cập; áp dụng biện pháp xác thực tăng cường đối với tài khoản quản trị, tài khoản có quyền truy cập dữ liệu cá nhân nhạy cảm và các trường hợp có mức độ rủi ro cao theo quy định.

Điều 10. Hỗ trợ người dùng

1. Trung tâm Thông tin y tế Quốc gia là đầu mối tổ chức hỗ trợ người sử dụng Hệ thống trên phạm vi toàn quốc; tổ chức tiếp nhận, hướng dẫn, hỗ trợ và điều phối xử lý các yêu cầu, phản ánh, sự cố phát sinh trong quá trình sử dụng Hệ thống.

2. Sở Y tế các tỉnh, thành phố trực thuộc Trung ương có trách nhiệm bố trí đầu mối hỗ trợ người sử dụng trên địa bàn; tiếp nhận, hướng dẫn, xử lý hoặc phối hợp xử lý các yêu cầu, vướng mắc thuộc phạm vi quản lý; trường hợp vượt quá phạm vi xử lý thì chuyển đến Trung tâm Thông tin y tế Quốc gia.

3. Các cơ sở khám bệnh, chữa bệnh, các đơn vị sử dụng Hệ thống có trách nhiệm bố trí đầu mối hướng dẫn người sử dụng trong đơn vị; tiếp nhận, kiểm tra, xác minh thông tin và phối hợp xử lý các yêu cầu, vướng mắc phát sinh trước khi đề nghị cơ quan cấp trên hỗ trợ.

4. Việc hỗ trợ người sử dụng được thực hiện thông qua tổng đài, thư điện tử, hệ thống tiếp nhận yêu cầu trực tuyến hoặc các hình thức khác do Bộ Y tế hoặc đơn vị quản lý Hệ thống công bố.

5. Đơn vị quản lý Hệ thống có trách nhiệm ban hành hoặc tổ chức thực hiện quy trình tiếp nhận, phân loại, chuyển xử lý, theo dõi và xác nhận kết quả giải quyết yêu cầu hỗ trợ; định kỳ tổng hợp, đánh giá tình hình và chất lượng hỗ trợ người sử dụng, báo cáo Bộ Y tế theo quy định.

6. Đối với các sự cố có nguy cơ ảnh hưởng đến hoạt động của Hệ thống hoặc việc kết nối, chia sẻ dữ liệu trên diện rộng, đơn vị quản lý Hệ thống chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tổ chức xử lý kịp thời nhằm bảo đảm Hệ thống hoạt động ổn định, liên tục. Trường hợp sự cố liên quan đến an ninh mạng, an ninh dữ liệu hoặc dữ liệu cá nhân thì thực hiện theo quy định tại Chương IV của Quy chế này.

7. Đơn vị vận hành Hệ thống có trách nhiệm tiếp nhận các yêu cầu được chuyển xử lý theo phạm vi nhiệm vụ được giao; thực hiện phân tích, xử lý kỹ thuật, cập nhật tình trạng và kết quả xử lý; phối hợp với đơn vị quản lý Hệ thống và các cơ quan, đơn vị có liên quan trong quá trình hỗ trợ người sử dụng.

CHƯƠNG III. KHAI THÁC, KẾT NỐI VÀ CHIA SẺ DỮ LIỆU

Điều 11. Nguyên tắc khai thác dữ liệu

1. Việc khai thác, sử dụng dữ liệu trên Hệ thống phải đúng mục đích, đúng đối tượng, đúng thẩm quyền, phù hợp với chức năng, nhiệm vụ và phạm vi được phân quyền; chỉ khai thác dữ liệu trong phạm vi cần thiết để thực hiện mục đích đã được xác định. Trường hợp chưa xác định được căn cứ pháp lý, mục đích, đối tượng hoặc phạm vi dữ liệu được phép khai thác thì không thực hiện việc khai thác, cung cấp hoặc chia sẻ dữ liệu.

2. Đối với hoạt động quản lý nhà nước, chỉ đạo, điều hành, thống kê, phân tích, dự báo, nghiên cứu và xây dựng chính sách, ưu tiên khai thác dữ liệu tổng hợp, dữ liệu thống kê, dữ liệu đã được khử nhận dạng hoặc dữ liệu không xác định chủ thể; việc khai thác dữ liệu có khả năng xác định cá nhân chỉ được thực hiện khi cần thiết và có căn cứ theo quy định của pháp luật.

3. Đối với hoạt động khám bệnh, chữa bệnh, phòng bệnh, chăm sóc và quản lý sức khỏe, việc khai thác dữ liệu sức khỏe cá nhân và các thông tin có liên quan phải tuân thủ quy định của pháp luật về khám bệnh, chữa bệnh, bảo vệ dữ liệu cá nhân và các quy định pháp luật có liên quan.

4. Hoạt động khai thác dữ liệu phải được kiểm soát, giám sát và lưu vết; bảo đảm tính toàn vẹn, bảo mật của dữ liệu và không làm ảnh hưởng đến hoạt động bình thường của Hệ thống. Việc ghi nhận, quản lý và khai thác nhật ký thực hiện theo quy định tại Điều 19 của Quy chế này.

Điều 12. Phạm vi, thẩm quyền khai thác dữ liệu

1. Dữ liệu trên Hệ thống được khai thác để phục vụ:

a) Công tác bảo vệ, chăm sóc và nâng cao sức khỏe nhân dân;

b) Công tác quản lý nhà nước về y tế, chỉ đạo, điều hành, thống kê, phân tích, dự báo, xây dựng chiến lược, quy hoạch, kế hoạch và chính sách trong lĩnh vực y tế;

c) Giải quyết thủ tục hành chính, cung cấp dịch vụ công và thực hiện các nhiệm vụ theo quy định của pháp luật;

d) Nghiên cứu khoa học, đào tạo và các mục đích khác khi có căn cứ theo quy định của pháp luật.

2. Đối với hoạt động quản lý nhà nước, chỉ đạo, điều hành, thống kê, phân tích, dự báo, nghiên cứu khoa học và đào tạo, ưu tiên sử dụng dữ liệu tổng hợp, dữ liệu thống kê, dữ liệu đã được khử nhận dạng hoặc dữ liệu không xác định chủ thể. Việc khai thác dữ liệu có khả năng xác định cá nhân chỉ được thực hiện khi cần thiết để thực hiện mục đích đã được xác định và có căn cứ theo quy định của pháp luật.

3. Thẩm quyền khai thác dữ liệu được thực hiện theo quy định của pháp luật và phân quyền của Hệ thống, cụ thể như sau:

a) Các đơn vị thuộc, trực thuộc Bộ Y tế được khai thác dữ liệu trong phạm vi cần thiết để thực hiện chức năng, nhiệm vụ, quyền hạn được giao và theo phạm vi được phân quyền trên Hệ thống. Việc khai thác dữ liệu có khả năng xác định cá nhân phải có căn cứ theo quy định của pháp luật và chỉ thực hiện trong phạm vi cần thiết cho nhiệm vụ cụ thể;

b) Trung tâm Thông tin y tế Quốc gia được khai thác dữ liệu trong phạm vi cần thiết để thực hiện nhiệm vụ quản lý Hệ thống và các nhiệm vụ được giao. Đơn vị vận hành Hệ thống chỉ được truy cập, xử lý dữ liệu trong phạm vi cần thiết để thực hiện nhiệm vụ vận hành, bảo trì, hỗ trợ kỹ thuật, bảo đảm chất lượng dữ liệu và các nhiệm vụ được giao; không được khai thác, sử dụng dữ liệu cho mục đích khác. Mọi hoạt động truy cập, xử lý dữ liệu sức khỏe cá nhân phải được phân quyền, kiểm soát và lưu vết;

c) Sở Y tế, Trạm Y tế, cơ sở khám bệnh, chữa bệnh và các cơ quan, đơn vị y tế khác được khai thác dữ liệu theo chức năng, nhiệm vụ, phạm vi quản lý, phạm vi chuyên môn và quyền được phân cấp, phân quyền trên Hệ thống theo quy định của pháp luật;

d) Cơ quan, tổ chức ngoài phạm vi quy định tại các điểm a, b và c khoản này chỉ được khai thác, tiếp nhận dữ liệu khi có căn cứ pháp lý, đúng thẩm quyền, xác định rõ mục đích, phạm vi, nhóm dữ liệu, phương thức khai thác và trách nhiệm bảo vệ dữ liệu; việc cung cấp, chia sẻ dữ liệu thực hiện theo Điều 14 của Quy chế này.

4. Quyền khai thác dữ liệu được thiết lập trên Hệ thống theo chức năng, nhiệm vụ, thẩm quyền, phạm vi quản lý và nhu cầu khai thác hợp pháp của từng cơ quan, tổ chức, cá nhân; tuân thủ nguyên tắc quyền tối thiểu và các quy định về quản lý tài khoản, phân quyền tại Điều 9 của Quy chế này.

5. Dữ liệu sức khỏe được tích hợp, chia sẻ và hiển thị trên ứng dụng VNeID chỉ bao gồm các nhóm dữ liệu, trường thông tin đã được Bộ Y tế hoặc cơ quan có thẩm quyền quy định, ban hành hoặc công bố để tích hợp, khai thác, sử dụng trên VNeID; việc hiển thị, khai thác và sử dụng phải đúng mục đích, đối tượng, phạm vi và bảo đảm quyền của chủ thể dữ liệu theo quy định của pháp luật.

Điều 13. Hình thức khai thác dữ liệu

1. Dữ liệu trên Hệ thống được khai thác thông qua các hình thức sau đây:

a) Khai thác trực tiếp trên Hệ thống thông qua tài khoản được cấp và phạm vi được phân quyền, bao gồm Bảng thông tin tổng hợp (Dashboard), báo cáo, thống kê và các chức năng khai thác dữ liệu khác;

b) Khai thác thông qua kết nối bằng API hoặc phương thức kết nối, liên thông khác theo quy định của Bộ Y tế và pháp luật có liên quan;

c) Khai thác thông qua việc cung cấp dữ liệu theo yêu cầu của cơ quan, người có thẩm quyền trên cơ sở xác định rõ căn cứ pháp lý, mục đích, phạm vi, nhóm dữ liệu, phương thức cung cấp và trách nhiệm của bên tiếp nhận dữ liệu;

d) Các hình thức khai thác khác theo quy định của pháp luật hoặc quyết định của cơ quan có thẩm quyền.

2. Việc lựa chọn hình thức khai thác dữ liệu phải phù hợp với mục đích, đối tượng, phạm vi phân quyền, tính chất của dữ liệu và căn cứ pháp lý của hoạt động khai thác; bảo đảm chỉ cung cấp, hiển thị hoặc cho phép truy cập dữ liệu trong phạm vi cần thiết để thực hiện mục đích đã được xác định.

3. Đơn vị quản lý Hệ thống có trách nhiệm tổ chức, quản lý và xác định các hình thức khai thác dữ liệu phù hợp với yêu cầu quản lý nhà nước, yêu cầu chuyên môn, phạm vi phân quyền và điều kiện kỹ thuật của Hệ thống; phối hợp với đơn vị vận hành Hệ thống triển khai các giải pháp kỹ thuật phục vụ khai thác dữ liệu.

Điều 14. Chia sẻ dữ liệu

1. Việc chia sẻ dữ liệu từ Hệ thống phải có căn cứ pháp lý, đúng mục đích, đúng đối tượng, đúng thẩm quyền, đúng phạm vi và chỉ trong mức cần thiết để thực hiện mục đích đã được xác định; đồng thời phải đáp ứng yêu cầu về an ninh mạng, an ninh dữ liệu và bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

2. Hệ thống thực hiện chia sẻ dữ liệu với các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, hệ thống thông tin và cơ sở dữ liệu của cơ quan, tổ chức theo quy định của pháp luật hoặc quyết định của cơ quan có thẩm quyền.

3. Việc cung cấp, chia sẻ dữ liệu sức khỏe cho cơ quan, tổ chức, cá nhân ngoài ngành y tế hoặc ngoài phạm vi khai thác đã được quy định chỉ được thực hiện khi xác định đầy đủ các nội dung sau đây:

a) Căn cứ pháp lý của việc cung cấp, chia sẻ dữ liệu;

b) Thẩm quyền của cơ quan, tổ chức, cá nhân yêu cầu và tiếp nhận dữ liệu;

c) Mục đích xử lý dữ liệu;

d) Nhóm dữ liệu, trường thông tin, phạm vi chủ thể dữ liệu và phạm vi dữ liệu cần cung cấp;

đ) Phương thức cung cấp, chia sẻ dữ liệu;

e) Thời hạn, phạm vi khai thác, sử dụng dữ liệu;

g) Biện pháp bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân và trách nhiệm của bên tiếp nhận dữ liệu.

4. Không thực hiện cung cấp, chia sẻ dữ liệu khi chưa xác định được căn cứ pháp lý, thẩm quyền, mục đích xử lý, phạm vi dữ liệu hoặc trách nhiệm của bên tiếp nhận dữ liệu. Trường hợp pháp luật quy định phải có sự đồng ý, yêu cầu hoặc chấp thuận của chủ thể dữ liệu thì việc cung cấp, chia sẻ chỉ được thực hiện sau khi đáp ứng đầy đủ điều kiện đó.

5. Đơn vị quản lý Hệ thống có trách nhiệm tổ chức quản lý, kiểm soát và giám sát hoạt động chia sẻ dữ liệu; phê duyệt hoặc tham mưu cấp có thẩm quyền phê duyệt việc chia sẻ dữ liệu theo thẩm quyền; bảo đảm hoạt động chia sẻ được ghi nhận, lưu vết và kịp thời áp dụng biện pháp ngăn chặn khi phát hiện việc khai thác, sử dụng dữ liệu không đúng quy định.

6. Cơ quan, tổ chức, cá nhân tiếp nhận dữ liệu có trách nhiệm sử dụng dữ liệu đúng mục đích, đúng phạm vi, đúng thẩm quyền và trong thời hạn được phép; áp dụng các biện pháp bảo vệ dữ liệu; không được mở rộng mục đích xử lý, phạm vi khai thác hoặc cung cấp, chia sẻ lại dữ liệu cho bên thứ ba nếu không có căn cứ pháp lý hoặc không được cơ quan có thẩm quyền cho phép theo quy định của pháp luật.

Điều 15. Kết nối, liên thông dữ liệu

1. Việc kết nối, liên thông dữ liệu với Hệ thống phải tuân thủ quy định của pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật, chuẩn dữ liệu, quy định về kết nối, chia sẻ dữ liệu và đặc tả kỹ thuật do Bộ Y tế ban hành; bảo đảm đúng mục đích, phạm vi kết nối được phê duyệt và các yêu cầu về an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân.

2. Cơ quan, tổ chức, đơn vị thực hiện kết nối với Hệ thống có trách nhiệm:

a) Bảo đảm dữ liệu gửi đến Hệ thống đúng cấu trúc, định dạng, đầy đủ, chính xác, hợp lệ và kịp thời theo quy định, hướng dẫn và đặc tả kỹ thuật của Bộ Y tế;

b) Bảo đảm an ninh mạng, an ninh dữ liệu và bảo vệ dữ liệu cá nhân đối với hệ thống thuộc phạm vi quản lý của mình trong quá trình kết nối, truyền nhận, đồng bộ dữ liệu;

c) Quản lý, bảo vệ tài khoản liên thông, thông tin xác thực và các thông tin kỹ thuật được cấp để thực hiện kết nối;

d) Theo dõi tình trạng kết nối, phối hợp với đơn vị quản lý Hệ thống và đơn vị vận hành Hệ thống trong xử lý lỗi, sự cố và bảo đảm chất lượng dữ liệu.

3. Đơn vị quản lý Hệ thống có trách nhiệm:

a) Ban hành hoặc trình cấp có thẩm quyền ban hành các quy định, quy trình, hướng dẫn và đặc tả kỹ thuật về kết nối, liên thông dữ liệu;

b) Tổ chức quản lý việc thiết lập, thay đổi, tạm dừng, chấm dứt kết nối; cấp, điều chỉnh, tạm khóa hoặc thu hồi quyền kết nối theo thẩm quyền;

c) Kiểm tra, giám sát hoạt động kết nối, liên thông dữ liệu; chủ trì phối hợp xử lý các khó khăn, vướng mắc và các trường hợp kết nối không đáp ứng yêu cầu.

4. Đơn vị vận hành Hệ thống có trách nhiệm:

a) Triển khai, duy trì các thành phần kỹ thuật phục vụ kết nối, liên thông dữ liệu theo yêu cầu của đơn vị quản lý Hệ thống;

b) Theo dõi, giám sát tình trạng kết nối, lưu lượng và kết quả truyền nhận dữ liệu; kịp thời phát hiện, cảnh báo, xử lý hoặc phối hợp xử lý các lỗi, sự cố kỹ thuật;

c) Hỗ trợ cơ quan, tổ chức, đơn vị trong quá trình thiết lập, kiểm thử, vận hành và duy trì kết nối;

d) Báo cáo đơn vị quản lý Hệ thống về tình trạng kết nối, sự cố, nguy cơ và các vấn đề phát sinh trong phạm vi nhiệm vụ được giao.

5. Cơ quan, tổ chức, địa phương có hệ thống hồ sơ sức khỏe điện tử, kho dữ liệu dùng chung, nền tảng tích hợp dữ liệu hoặc hệ thống trung gian đáp ứng yêu cầu của Bộ Y tế có thể thực hiện kết nối với Hệ thống thông qua nền tảng hoặc hệ thống trung gian đó theo hướng dẫn của Bộ Y tế, sau khi đáp ứng đầy đủ các điều kiện về kết nối, chia sẻ dữ liệu theo quy định của pháp luật và Quy chế này.

6. Việc kết nối thông qua nền tảng tích hợp hoặc hệ thống trung gian không làm thay đổi trách nhiệm của cơ quan, tổ chức, đơn vị tạo lập, cung cấp dữ liệu đối với tính chính xác, đầy đủ, kịp thời, hợp pháp và chất lượng của dữ liệu gửi đến Hệ thống.

7. Việc kết nối, liên thông Cổng dữ liệu sức khỏe với Hệ thống định danh và xác thực điện tử, ứng dụng VNeID phải đáp ứng đầy đủ các yêu cầu về an ninh mạng theo cấp độ của Hệ thống và các yêu cầu, giải pháp bảo đảm an toàn, an ninh mạng phục vụ kết nối theo Công văn số 708/BTTTT-CATTT ngày 02 tháng 3 năm 2024 của Bộ Thông tin và Truyền thông, các quy định pháp luật hiện hành và văn bản sửa đổi, bổ sung, thay thế hoặc hướng dẫn có liên quan của cơ quan có thẩm quyền.

Điều 16. Đối soát và xử lý sai lệch dữ liệu

1. Việc đối soát dữ liệu được thực hiện nhằm phát hiện, xác minh và xử lý các trường hợp dữ liệu sai, thiếu, không thống nhất hoặc không khớp giữa dữ liệu trên Hệ thống với dữ liệu tại nguồn và dữ liệu trên ứng dụng VNeID; bảo đảm tính chính xác, đầy đủ, thống nhất, kịp thời và toàn vẹn của dữ liệu.

2. Khi phát hiện dữ liệu của cùng một chủ thể có sự khác biệt, mâu thuẫn hoặc sai lệch giữa các nguồn dữ liệu, việc đối soát và xử lý được thực hiện như sau:

a) Đơn vị quản lý Hệ thống chủ trì hoặc điều phối việc đối soát, phối hợp với các cơ quan, tổ chức, đơn vị có liên quan để xác minh nguyên nhân và xác định phương án xử lý;

b) Đơn vị vận hành Hệ thống thực hiện các biện pháp kỹ thuật phục vụ đối soát, kiểm tra, cập nhật, đồng bộ dữ liệu theo yêu cầu của đơn vị quản lý Hệ thống;

c) Cơ quan, tổ chức, đơn vị tạo lập, cung cấp và hiển thị dữ liệu có trách nhiệm kiểm tra, xác minh, cung cấp thông tin và thực hiện việc chỉnh sửa dữ liệu thuộc phạm vi quản lý của mình theo quy định.

3. Việc chỉnh sửa dữ liệu sau đối soát phải ưu tiên thực hiện tại hệ thống hoặc cơ sở dữ liệu nguồn; Hệ thống cập nhật, đồng bộ theo dữ liệu nguồn đã được chỉnh sửa hoặc theo kết quả xác nhận của cơ quan, tổ chức có thẩm quyền. Mọi hoạt động chỉnh sửa, cập nhật dữ liệu phải được ghi nhận và lưu vết theo quy định.

4. Cơ quan, tổ chức, đơn vị tạo lập hoặc cung cấp dữ liệu có trách nhiệm chủ động phối hợp đối soát, xác minh và chỉnh sửa dữ liệu thuộc phạm vi quản lý khi phát hiện sai lệch hoặc theo yêu cầu của cơ quan có thẩm quyền.

CHƯƠNG IV. BẢO ĐẢM AN NINH MẠNG, AN NINH DỮ LIỆU VÀ BẢO VỆ DỮ LIỆU CÁ NHÂN

Điều 17. Nguyên tắc bảo đảm an ninh mạng, an ninh dữ liệu và bảo vệ dữ liệu cá nhân

1. Việc quản lý, vận hành và sử dụng Hệ thống; thu thập, lưu trữ, xử lý, khai thác, kết nối, chia sẻ dữ liệu phải được bảo đảm an ninh mạng, an ninh dữ liệu và bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

2. Dữ liệu sức khỏe là dữ liệu cá nhân nhạy cảm; việc xử lý dữ liệu sức khỏe phải tuân thủ quy định của pháp luật về bảo vệ dữ liệu cá nhân và các quy định pháp luật có liên quan.

3. Việc xử lý dữ liệu sức khỏe phải đúng mục đích, đúng đối tượng, đúng thẩm quyền và trong phạm vi cần thiết; tuân thủ nguyên tắc tối thiểu hóa dữ liệu. Không thu thập, lưu trữ, khai thác, sử dụng hoặc chia sẻ dữ liệu vượt quá phạm vi cần thiết cho mục đích xử lý đã được xác định. Thời hạn lưu trữ dữ liệu thực hiện theo quy định của pháp luật và phù hợp với mục đích xử lý.

4. Hệ thống phải được xác định, phê duyệt cấp độ và triển khai đầy đủ các biện pháp bảo đảm an ninh mạng tương ứng với cấp độ theo quy định của pháp luật; áp dụng TCVN 14423:2026 An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản và các tiêu chuẩn, quy chuẩn kỹ thuật có liên quan trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp và bảo vệ Hệ thống.

Điều 18. Bảo đảm an ninh mạng và ứng cứu sự cố

1. Đơn vị quản lý Hệ thống có trách nhiệm:

a) Tổ chức xác định, rà soát cấp độ Hệ thống; xây dựng, ban hành hoặc trình cấp có thẩm quyền ban hành phương án, quy trình và các yêu cầu bảo đảm an ninh mạng theo quy định;

b) Tổ chức giám sát, phát hiện, cảnh báo nguy cơ, mối đe dọa, sự cố an ninh mạng; chủ trì điều phối việc ứng cứu, khắc phục và phục hồi hoạt động của Hệ thống;

c) Tham mưu, tổ chức thực hiện việc kết nối hệ thống giám sát an ninh mạng, hệ thống phòng, chống mã độc tập trung của Hệ thống với Trung tâm An

ninh mạng quốc gia của Bộ Công an hoặc Trung tâm An ninh mạng của tỉnh, thành phố theo quy định của pháp luật; thực hiện chia sẻ thông tin, cảnh báo và phối hợp giám sát, phát hiện, ngăn chặn, xử lý nguy cơ, mối đe dọa, sự cố an ninh mạng;

d) Tiếp nhận, tổng hợp, báo cáo thông tin về nguy cơ, mối đe dọa, sự cố an ninh mạng; thực hiện chế độ thông báo, báo cáo theo quy định của pháp luật;

đ) Hướng dẫn, kiểm tra, giám sát việc thực hiện các yêu cầu về an ninh mạng đối với các cơ quan, tổ chức, đơn vị tham gia quản lý, vận hành, kết nối, khai thác và sử dụng Hệ thống.

2. Đơn vị vận hành Hệ thống có trách nhiệm:

a) Triển khai các biện pháp quản lý, biện pháp kỹ thuật bảo đảm an ninh mạng trong phạm vi nhiệm vụ được giao theo phương án, yêu cầu của đơn vị quản lý Hệ thống;

b) Theo dõi, giám sát, phát hiện, cảnh báo và xử lý ban đầu đối với các nguy cơ, mối đe dọa, sự cố an ninh mạng; ghi nhận và lưu giữ nhật ký hệ thống theo quy định;

c) Phối hợp với đơn vị quản lý Hệ thống và các cơ quan, tổ chức có liên quan trong việc ứng cứu, khắc phục, phục hồi hoạt động của Hệ thống;

d) Thực hiện các yêu cầu kỹ thuật phục vụ kết nối, duy trì kết nối và chia sẻ thông tin giữa hệ thống giám sát an ninh mạng, hệ thống phòng, chống mã độc tập trung của Hệ thống với cơ quan, đơn vị có thẩm quyền theo yêu cầu của đơn vị quản lý Hệ thống và quy định của pháp luật.

3. Cơ sở khám bệnh, chữa bệnh, cơ quan, tổ chức, đơn vị tham gia kết nối, chia sẻ, khai thác và sử dụng Hệ thống có trách nhiệm thực hiện các biện pháp bảo đảm an ninh mạng đối với hệ thống thuộc phạm vi quản lý; kịp thời thông báo khi phát hiện nguy cơ, mối đe dọa hoặc sự cố; phối hợp cung cấp thông tin, tài liệu và thực hiện các yêu cầu phục vụ ứng cứu, điều tra, khắc phục, xử lý sự cố theo quy định.

4. Đối với sự cố có nguy cơ hoặc đã gây ảnh hưởng đến dữ liệu cá nhân, các cơ quan, tổ chức, đơn vị có liên quan phải kịp thời áp dụng biện pháp ngăn chặn, hạn chế thiệt hại, khắc phục, phối hợp xử lý, thông báo, báo cáo và thực hiện các nghĩa vụ khác theo quy định của pháp luật.

5. Việc kiểm tra, đánh giá an ninh mạng đối với Hệ thống được thực hiện định kỳ, khi có yêu cầu của cơ quan có thẩm quyền, khi có thay đổi lớn về kiến trúc, chức năng, phạm vi kết nối, khi nâng cấp, mở rộng Hệ thống hoặc khi xảy ra sự cố có nguy cơ ảnh hưởng đến an ninh mạng theo quy định của pháp luật.

Điều 19. Bảo vệ dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân trên Hệ thống phải tuân thủ quy định của pháp luật về bảo vệ dữ liệu cá nhân, dữ liệu, khám bệnh, chữa bệnh và các quy định pháp luật có liên quan.

2. Cơ quan, tổ chức, đơn vị và cá nhân tham gia quản lý, vận hành, tạo lập, khai thác, sử dụng hoặc xử lý dữ liệu trên Hệ thống chỉ được xử lý dữ liệu cá nhân khi có căn cứ pháp lý, đúng mục đích, đúng thẩm quyền và trong phạm vi cần thiết để thực hiện chức năng, nhiệm vụ hoặc mục đích xử lý đã được xác định; chịu trách nhiệm trước pháp luật đối với hoạt động xử lý dữ liệu thuộc phạm vi của mình.

3. Đơn vị quản lý Hệ thống có trách nhiệm tổ chức triển khai các biện pháp quản lý bảo vệ dữ liệu cá nhân; kiểm tra, giám sát hoạt động xử lý dữ liệu; ban hành hoặc tổ chức thực hiện quy trình kiểm soát truy cập, khai thác, chia sẻ, ghi nhận và lưu vết; phối hợp xử lý yêu cầu, phản ánh, vi phạm và sự cố liên quan đến dữ liệu cá nhân.

4. Đơn vị vận hành Hệ thống có trách nhiệm triển khai, duy trì các biện pháp kỹ thuật bảo vệ dữ liệu cá nhân theo yêu cầu của đơn vị quản lý Hệ thống; không được truy cập, khai thác hoặc sử dụng dữ liệu cho mục đích ngoài nhiệm vụ được giao.

5. Các biện pháp kỹ thuật bảo vệ dữ liệu cá nhân trên Hệ thống tối thiểu bao gồm các biện pháp về kiểm soát truy cập, mã hóa, ghi nhật ký, kiểm soát trích xuất, khử nhận dạng hoặc ẩn danh, phân tách môi trường, xóa hủy an toàn, kiểm tra đánh giá định kỳ và các biện pháp khác theo quy định.

6. Mọi hoạt động truy cập, khai thác, cập nhật, chỉnh sửa, trích xuất, cung cấp, kết nối, chia sẻ và các hoạt động xử lý khác đối với dữ liệu sức khỏe phải được kiểm soát, ghi nhận và lưu vết; bảo đảm khả năng xác định chủ thể thực hiện, thời điểm, loại hoạt động, đối tượng hoặc phạm vi dữ liệu được xử lý, bên tiếp nhận và kết quả thực hiện. Nhật ký phải được bảo vệ khỏi việc truy cập, sửa đổi, xóa hoặc hủy trái phép.

7. Việc lập, quản lý, cập nhật hồ sơ xử lý dữ liệu cá nhân; chỉ định nhân sự hoặc bộ phận bảo vệ dữ liệu cá nhân; đánh giá tác động xử lý dữ liệu cá nhân; tiếp nhận, giải quyết yêu cầu của chủ thể dữ liệu và thực hiện các nghĩa vụ khác về bảo vệ dữ liệu cá nhân được thực hiện theo quy định của pháp luật.

Chương V. TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC

Điều 20. Trách nhiệm của Trung tâm Thông tin y tế Quốc gia

Trung tâm Thông tin y tế Quốc gia là đơn vị quản lý Hệ thống và có trách nhiệm:

1. Chủ trì quản lý, tổ chức vận hành, duy trì và phát triển Hệ thống; bảo

đảm Hệ thống hoạt động ổn định, liên tục, an toàn theo quy định của pháp luật và Quy chế này.

2. Chủ trì tổ chức kết nối, tích hợp, đồng bộ, chia sẻ và đối soát dữ liệu giữa Hệ thống với các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, hệ thống thông tin và cơ sở dữ liệu có liên quan theo quy định của pháp luật; tổ chức thực hiện theo các quy định tại Chương III của Quy chế này.

3. Tổ chức cập nhật, hoàn thiện, nâng cấp và phát triển Hệ thống phù hợp với yêu cầu quản lý, yêu cầu chuyên môn, quy định của pháp luật và nhu cầu thực tiễn.

4. Hướng dẫn, hỗ trợ các cơ quan, tổ chức, đơn vị và cá nhân trong quá trình triển khai, kết nối, cập nhật, khai thác và sử dụng Hệ thống theo phạm vi chức năng, nhiệm vụ được giao.

5. Chủ trì xây dựng, ban hành hoặc trình cấp có thẩm quyền ban hành các quy trình, hướng dẫn và tài liệu phục vụ quản lý, vận hành, kết nối, khai thác, chia sẻ dữ liệu và bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân của Hệ thống.

6. Theo dõi, kiểm tra, tổng hợp tình hình quản lý, vận hành, kết nối, cập nhật, khai thác và chia sẻ dữ liệu của Hệ thống; định kỳ hoặc đột xuất báo cáo Bộ Y tế theo quy định.

7. Là đầu mối phối hợp với các đơn vị thuộc, trực thuộc Bộ Y tế, Sở Y tế, cơ sở khám bệnh, chữa bệnh, cơ quan quản lý dữ liệu có liên quan và các đơn vị khác trong quá trình quản lý, vận hành, khai thác, kết nối, chia sẻ và xử lý các vấn đề phát sinh đối với Hệ thống.

Điều 21. Trách nhiệm của các đơn vị thuộc, trực thuộc Bộ Y tế

Các đơn vị thuộc, trực thuộc Bộ Y tế, trong phạm vi chức năng, nhiệm vụ và quyền hạn được giao, có trách nhiệm:

1. Chủ trì hoặc phối hợp xây dựng, hướng dẫn, cập nhật các quy định, quy trình chuyên môn, yêu cầu nghiệp vụ, danh mục và yêu cầu chất lượng dữ liệu sức khỏe thuộc lĩnh vực được giao; hướng dẫn việc thu thập, tạo lập, cập nhật, khai thác và sử dụng dữ liệu theo quy định của pháp luật.

2. Phối hợp với Trung tâm Thông tin y tế Quốc gia trong việc xây dựng, hoàn thiện, nâng cấp và phát triển Hệ thống; xác định, cung cấp và xác nhận các yêu cầu nghiệp vụ, yêu cầu chuyên môn thuộc lĩnh vực phụ trách.

3. Khai thác, sử dụng dữ liệu trên Hệ thống trong phạm vi chức năng, nhiệm vụ, quyền hạn và phạm vi được phân quyền để phục vụ quản lý nhà nước, chỉ đạo, điều hành, thống kê, phân tích, dự báo và xây dựng chính sách theo quy định tại Chương III của Quy chế này.

4. Chủ trì hoặc phối hợp kiểm tra, giám sát việc thực hiện các quy định chuyên môn, nghiệp vụ và yêu cầu về dữ liệu thuộc lĩnh vực được giao; phối hợp

với Trung tâm Thông tin y tế Quốc gia trong việc kiểm tra thực hiện Quy chế này theo phạm vi chức năng, nhiệm vụ.

Điều 22. Trách nhiệm của Sở Y tế

1. Chỉ đạo các cơ quan, đơn vị thuộc phạm vi quản lý bảo đảm nhân lực, hạ tầng kỹ thuật và các điều kiện cần thiết để triển khai, kết nối, cập nhật, khai thác và sử dụng Hệ thống theo quy định.

2. Tổ chức hướng dẫn, hỗ trợ người sử dụng theo phân cấp; đôn đốc, kiểm tra, giám sát các cơ sở khám bệnh, chữa bệnh và các đơn vị có liên quan trong triển khai Hệ thống.

3. Theo dõi, giám sát tình hình cập nhật và chất lượng dữ liệu của các cơ sở khám bệnh, chữa bệnh trên địa bàn; hướng dẫn, đôn đốc và phối hợp xử lý các sai sót, bảo đảm dữ liệu đầy đủ, chính xác, kịp thời và đúng quy định.

4. Khai thác, sử dụng dữ liệu trên Hệ thống trong phạm vi chức năng, nhiệm vụ, quyền hạn, phạm vi quản lý và phạm vi được phân quyền để phục vụ công tác quản lý nhà nước về y tế trên địa bàn theo quy định tại Chương III của Quy chế này.

5. Tổng hợp, đánh giá tình hình triển khai, cập nhật, kết nối và chất lượng dữ liệu trên địa bàn; thực hiện chế độ báo cáo Bộ Y tế theo quy định.

Điều 23. Trách nhiệm của các cơ sở khám bệnh, chữa bệnh

1. Bảo đảm nhân lực, hạ tầng kỹ thuật, phần mềm và các điều kiện cần thiết để thực hiện việc tạo lập, cập nhật, kết nối, chia sẻ, khai thác và sử dụng dữ liệu trên Hệ thống theo quy định.

2. Thu thập, tạo lập, cập nhật, kết nối và chia sẻ dữ liệu sức khỏe thuộc phạm vi trách nhiệm của cơ sở theo đúng quy định của pháp luật, quy định chuyên môn, chuẩn dữ liệu và yêu cầu kỹ thuật của Bộ Y tế. Thực hiện ký số đối với dữ liệu, hồ sơ điện tử thuộc trường hợp phải ký số theo quy định của pháp luật.

3. Chịu trách nhiệm về tính chính xác, đầy đủ, kịp thời, hợp pháp và chất lượng của dữ liệu do cơ sở tạo lập, cập nhật, cung cấp hoặc chia sẻ lên Hệ thống; bảo đảm dữ liệu "đúng, đủ, sạch, sống".

4. Khi phát hiện hoặc nhận được thông tin về dữ liệu sai, thiếu, không khớp hoặc cần đối soát, cơ sở có trách nhiệm kịp thời kiểm tra, xác minh; thực hiện chỉnh sửa dữ liệu thuộc phạm vi quản lý tại nguồn và cập nhật, đồng bộ lại lên Hệ thống. Không được tự ý sửa đổi dữ liệu không do cơ sở tạo lập hoặc dữ liệu thuộc nguồn quản lý của cơ quan, tổ chức khác.

5. Quản lý, sử dụng tài khoản và quyền truy cập đúng mục đích, đúng đối tượng, đúng phạm vi được phân quyền; thực hiện các yêu cầu về an ninh mạng, an ninh dữ liệu và bảo vệ dữ liệu cá nhân theo quy định tại Chương IV của Quy chế này và pháp luật có liên quan.

6. Kịp thời thông báo cho Trung tâm Thông tin y tế Quốc gia, Sở Y tế hoặc

cơ quan có thẩm quyền theo quy định khi phát hiện sự cố kỹ thuật, nguy cơ hoặc sự cố an ninh mạng, mất an ninh dữ liệu, vi phạm hoặc sự cố liên quan đến dữ liệu cá nhân có ảnh hưởng đến Hệ thống; phối hợp xử lý, khắc phục và thực hiện chế độ báo cáo theo quy định.

Chương VI. ĐIỀU KHOẢN THI HÀNH

Điều 24. Tổ chức thực hiện

1. Trung tâm Thông tin y tế Quốc gia là đầu mối hướng dẫn, theo dõi, đôn đốc và tổng hợp tình hình thực hiện Quy chế này.

2. Thủ trưởng các cơ quan, tổ chức, đơn vị thuộc phạm vi áp dụng của Quy chế này có trách nhiệm tổ chức thực hiện đầy đủ các quy định của Quy chế trong phạm vi chức năng, nhiệm vụ, quyền hạn được giao và chịu trách nhiệm về việc thực hiện tại cơ quan, tổ chức, đơn vị mình.

3. Trong quá trình thực hiện, trường hợp phát sinh khó khăn, vướng mắc, cơ quan, tổ chức, đơn vị phản ánh về Trung tâm Thông tin y tế Quốc gia để tổng hợp, phối hợp xử lý hoặc báo cáo Bộ Y tế xem xét, quyết định theo thẩm quyền. Đối với nội dung thuộc lĩnh vực chuyên môn, Trung tâm Thông tin y tế Quốc gia phối hợp với đơn vị thuộc, trực thuộc Bộ Y tế phụ trách lĩnh vực đó và các cơ quan, tổ chức có liên quan để tham mưu xử lý.

Điều 25. Điều khoản tham chiếu

Trường hợp các văn bản được dẫn chiếu trong Quy chế này được sửa đổi, bổ sung hoặc thay thế thì áp dụng theo văn bản sửa đổi, bổ sung, thay thế đó.