

BỘ Y TẾ

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

Số: 5689/BYT- K2ĐT

V/v rà soát, thực hiện các biện pháp
bảo đảm an ninh mạng, an ninh dữ liệu,
bảo vệ dữ liệu cá nhân và phòng chống
lộ lọt dữ liệu ngành y tế

Hà Nội, ngày 30 tháng 7 năm 2026

Kính gửi:

- Các cơ quan, đơn vị thuộc, trực thuộc Bộ Y tế;
 - Các Sở Y tế tỉnh/thành phố trực thuộc TW.
- (Sau đây gọi là các Đơn vị)

Theo thông tin được công bố tại một số văn bản của Bộ Công an¹, hiện nay tình trạng tấn công mạng và rò rỉ dữ liệu tại Việt Nam đang ở mức báo động, đặc biệt trong giai đoạn 2023-2025 đã ghi nhận hơn 14,5 triệu tài khoản bị lộ và hơn 160 triệu bản ghi có liên quan dữ liệu cá nhân bị lộ lọt, dẫn đến hệ lụy khoảng gần 40.000 tỷ đồng bị chiếm đoạt, thông tin cá nhân bị khai thác trái phép, đồng thời ảnh hưởng đến uy tín, danh dự của nhiều cơ quan, tổ chức. Trong thời gian qua, Bộ Công an và Bộ Y tế đã ghi nhận một số Hệ thống thông tin (HTTT) và Cơ sở dữ liệu (CSDL) quan trọng của Bộ Y tế, ngành y tế cũng đã xảy ra tình trạng mất an toàn, an ninh thông tin, lộ lọt dữ liệu ở mức nghiêm trọng, ảnh hưởng đến an ninh, an toàn thông tin và dữ liệu.

Ngành y tế với đặc thù phải xây dựng, triển khai, quản lý, lưu trữ và vận hành nhiều CSDL và dữ liệu nhạy cảm của cá nhân, do vậy ngành đang đối mặt với nguy cơ tấn công nhằm đánh cắp dữ liệu, dữ liệu nhạy cảm và có thể gây thất thoát thông tin, dữ liệu rất lớn nếu không được phân loại và triển khai đầy đủ các biện pháp bảo vệ theo quy định. Thực hiện Luật An ninh mạng năm 2025; Luật Bảo vệ dữ liệu cá nhân năm 2025; Luật Dữ liệu năm 2024; Luật Khám bệnh, chữa bệnh năm 2023, Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị, Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số; Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị, Bộ Y tế đề nghị Thủ trưởng các đơn vị khẩn trương rà soát, thực hiện các nội dung sau đây để tăng cường công tác bảo đảm an ninh mạng, an ninh dữ liệu và bảo vệ dữ liệu cá nhân tại các HTTT, CSDL, kho dữ liệu về y tế tại đơn vị:

¹ Công văn số 3461/BCA-A05 ngày 03/7/2026 của Bộ Công an về việc nguy cơ mất an ninh mạng Hệ thống thông tin y tế; Công văn số 2656/BCA-A05 ngày 02/6/2026 của Bộ Công an về việc hướng dẫn triển khai công tác bảo đảm an ninh mạng, an ninh thông tin, an ninh dữ liệu.

1. Rà soát, đánh giá và phân loại hệ thống thông tin, phân loại dữ liệu

- Thực hiện rà soát, xác định cấp độ an ninh và lập hồ sơ đề xuất, phương án bảo đảm an ninh thông tin theo cấp độ của HTTT, CSDL (từ cấp độ 1 đến cấp độ 5) do đơn vị quản lý; phân loại dữ liệu của các HTTT, CSDL và triển khai các biện pháp bảo đảm, bảo vệ theo quy định.

- Sử dụng tiêu chuẩn quốc gia TCVN 14423:2025 làm cơ sở để đánh giá toàn diện, thiết lập, bổ sung các tiêu chí chưa tuân thủ quy định về an ninh mạng, bảo mật thông tin và an ninh dữ liệu đối với HTTT, CSDL.

- Lập danh mục và phân loại tất cả tài sản về phần cứng, phần mềm và dữ liệu y tế để xây dựng phương án bảo vệ "đúng, đủ", tránh đầu tư "dàn trải, lãng phí"

2. Các giải pháp quản lý bảo đảm an ninh, an toàn thông tin

- Ban hành và thường xuyên rà soát cập nhật quy chế, chính sách bảo đảm an ninh mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp, hủy bỏ HTTT, CSDL; làm rõ trách nhiệm của từng cá nhân đối trong công tác quản lý, vận hành các HTTT, CSDL của đơn vị.

- Thực hiện kiểm tra, đánh giá an ninh thông tin cho các HTTT, CSDL trước khi đưa vào sử dụng và đánh giá an ninh định kỳ độc lập (02 năm/lần đối với các HTTT cấp độ 1, 2; hàng năm đối với HTTT cấp độ 3, 4; 06 tháng/lần đối với HTTT cấp độ 5).

- Tổ chức, tham gia đào tạo, tập huấn nâng cao trình độ chuyên môn về an ninh thông tin, an ninh dữ liệu cho cán bộ kỹ thuật và nâng cao nhận thức ATTT người dùng để giảm thiểu rủi ro lộ lọt dữ liệu liên quan đến người dùng.

3. Một giải pháp kỹ thuật quan trọng trong phòng chống lộ lọt dữ liệu

a) Chuẩn hóa mô hình mạng và triển khai phương án kỹ thuật đảm bảo an ninh thông tin:

- Phân chia vùng mạng theo chức năng (vùng nội bộ, vùng DMZ, vùng máy chủ dữ liệu...);

- Áp dụng nguyên tắc "đặc quyền tối thiểu" để hạn chế bề mặt tấn công, tấn công leo thang, lây lan mã độc và dễ dàng cô lập vùng mạng khi có sự cố; triển khai đầy đủ phương án đảm bảo an ninh thông tin theo hồ sơ cấp độ được phê duyệt.

b) Bảo vệ người dùng cuối:

- Triển khai đầy đủ phương án phòng chống mã độc, phòng chống thất thoát dữ liệu, giám sát an ninh thông tin trên máy trạm xử lý dữ liệu của người dùng cuối;

- Cán bộ có tài khoản xử lý dữ liệu trên các HTTT, CSDL phải chịu trách nhiệm bảo mật với tài khoản được cấp.

c) Giám sát và ứng cứu:

- Thiết lập hệ thống giám sát an ninh mạng 24/7 để phát hiện sớm các hành vi xâm nhập trái phép;
- Thường xuyên rà quét, cập nhật bản vá lỗ hổng bảo mật cho hệ điều hành, ứng dụng và CSDL của các HTTT.

d) Bảo vệ dữ liệu:

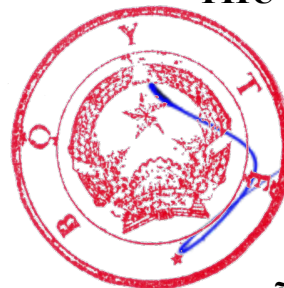
- Cần phân loại, gán nhãn dữ liệu theo mức độ quan trọng, nhạy cảm ngay từ khâu tạo lập; Thiết lập cứng hóa, cấp phát quyền kết nối, truy xuất cơ sở dữ liệu đúng vai trò, tuân thủ nguyên tắc đặc quyền tối thiểu;
- Đơn vị quản trị hệ thống chủ động rà soát, loại bỏ các tài khoản quản trị CSDL dư thừa, các tài khoản quản trị từ xa có quyền vào vùng mạng máy chủ CSDL, gán trách nhiệm với cán bộ nắm giữ tài khoản của HTTT, CSDL;
- Sử dụng các phương án mã hóa dữ liệu khi truyền đưa trên mạng (*data in transit*) và dữ liệu tĩnh trong lưu trữ (*data at rest*);
- Thiết lập hệ thống sao lưu dự phòng dữ liệu tách biệt hoàn toàn với hệ thống chính để sẵn sàng phục hồi khi gặp sự cố và phòng ngừa tấn công mã hóa dữ liệu;
- Đánh giá toàn diện các API ứng dụng có chức năng kết nối, truy xuất cơ sở dữ liệu nhằm phát hiện các lỗ hổng bảo mật về xác thực, phân quyền và dư thừa dữ liệu;
- Khuyến nghị triển khai giải pháp phòng chống thất thoát dữ liệu tập trung (DLP) trên toàn bộ hệ thống, máy trạm xử lý dữ liệu và thiết lập chính sách kiểm soát đúng với dữ liệu đã được phân loại, gán nhãn nhằm kiểm soát việc di chuyển dữ liệu nhạy cảm ra ngoài;
- Thực hiện nghiêm quy trình xóa và tiêu hủy thiết bị an toàn khi không còn nhu cầu sử dụng hoặc thay đổi mục đích sử dụng.

Bộ Y tế đề nghị các Đơn vị khẩn trương tổ chức thực hiện để bảo đảm bảo đảm an ninh mạng, an ninh dữ liệu và bảo vệ dữ liệu cá nhân tại các HTTT, CSDL, kho dữ liệu về y tế tại đơn vị./.

Nơi nhận:

- Như trên;
- Bộ Công an (để p/h);
- Bộ trưởng (để b/c);
- Các đ/c Thứ trưởng BYT (để p/h);
- Trung tâm TTYTQG;
- Lưu: VT, K2ĐT.

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**



Nguyễn Tri Thức