BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 272 /CNTT-CSHT
V/v Tăng cường đảm bảo an toàn dữ liệu số trên môi trường mạng

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

Hà Nội, ngày 18 tháng 5 năm 2018

Kính gửi:
- Các Vụ, Cục, Tổng cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Sở Y tế các tỉnh, thành phố trực thuộc Trung ương.
- Trung tâm tích hợp dữ liệu, Cục Công nghệ thông tin

Cục Công nghệ thông tin nhận được nhiều cảnh bảo về nguy cơ mất an toàn dữ liệu được quản lý, lưu trữ, truyền tải thông tin trên môi trường mạng. Để đảm bảo an toàn các thông tin bí mật theo quy định của nhà nước, theo quy định của Bộ Y tế và các thông tin quan trọng của đơn vị, Cục Công nghệ thông tin đề nghị các đơn vị nghiêm túc thực hiện các biện pháp sau:

1. Phân loại, xây dựng quy trình quản lý thông tin: Phân loại, xác định các thông tin y tế thuộc phạm vi bí mật theo quy định của nhà nước, của Bộ Y tế và các thông tin quan trọng của đơn vị. Xây dựng quy định quản lý, khai thác các dữ liệu này trên trên môi trường mạng.
2. Trước mắt tổ chức thực hiện các biện pháp đảm bảo an toàn, bảo mật thông tin cho các dữ liệu trên, cụ thể:

a) Bảo vệ thiết bị

- Thực hiện các biện pháp bảo vệ vật lý (như có cửa bảo vệ, có cán bộ bảo vệ …) khu vực đặt các thiết bị máy tính quản lý, lưu trữ dữ liệu.

- Thực hiện các biện pháp bảo vệ phòng máy chủ quản lý, lưu trữ dữ liệu theo hướng dẫn tại điều 6 tại Quyết định 4159/QĐ-BYT ngày 13/10/2014 của Bộ Y tế ban hành quy định về đảm bảo an toàn thông tin y tế điện tử tại các đơn vị trong ngành y tế.

- Thực hiện kiểm tra đối với việc mang thiết bị vào và thiết bị ra đối với phòng máy chủ quản lý, lưu trữ dữ liệu theo quy định tại điểm b, điểm c, mục 1, phần III tại quyết định 4495/QĐ-BYT ngày 30/10/2015 của Bộ trưởng Bộ y tế về việc ban hành hướng dẫn xây dựng nội quy an toàn, an ninh thông tin trong các đơn vị trong ngành y tế đối với phòng máy chủ lưu trữ dữ liệu.

- Không được chụp ảnh, quay camera các thiết bị tại phòng máy chủ quản lý, lưu trữ dữ liệu khi không được sự đồng ý bằng văn bản của lãnh đạo đơn vị.

- Thực hiện việc hủy bỏ các thiết bị lưu trữ thông tin y tế theo hướng dẫn tại điều 15 tại Quyết định 4159/QĐ-BYT ngày 13/10/2014 của Bộ Y tế ban hành quy định về đảm bảo an toàn thông tin y tế điện tử tại các đơn vị trong ngành y tế.

- Cài đặt các phần mềm hoặc thiết bị bảo vệ chống truy cập trái phép đối với các máy tính cá nhân sử dụng trong việc quản lý, lưu trữ, khai thác dữ liệu.

- Các thiết bị mạng đưa vào hoạt động hoặc rời khỏi mạng liên quan tới dữ liệu phải được sự đồng ý bằng văn bản của lãnh đạo đơn vị.

b) Bảo vệ dữ liệu

Thực hiện các biện pháp quản lý việc truy cập dữ liệu, cụ thể:

- Chỉ tạo tạo tài khoản truy cập và gán quyền truy cập cho các nhóm, cá nhận được phép truy cập vào dữ liệu theo quy định của đơn vị và của pháp luật;

- Ngừng ngay lập tức tài khoản truy cập đối với nhóm, cá nhân không còn được phép truy cập vào dữ liệu;

- Xây dựng cơ chế kiểm soát việc truy cập vật lý và trực tuyến đối với dữ liệu theo điểm a, điểm đ, mục 1; điểm a, điểm b, điểm c, điểm đ mục 2, phần III tại quyết định 4495/QĐ-BYT ngày 30/10/2015 của Bộ trưởng Bộ y tế về việc ban hành hướng dẫn xây dựng nội quy an toàn, an ninh thông tin trong các đơn vị trong ngành y tế.

Đối với các hệ thống thông tin khai thác dữ liệu:

- Xây dựng cơ chế kiểm soát truy cập vào hệ thống dựa trên vai trò (Role-based Access Control);

- Áp dụng biện pháp xác thực hai yếu tố khi truy cập vào dữ liệu;

- Áp dụng các biện pháp xác thực, mã hóa, chữ ký số khi gửi và nhận dữ liệu;

- Thực hiện quản lý tài khoản truy cập của người sử dụng theo quy định tại điều 13, chương II tại quyết định 4159/QĐ-BYT ngày 13/10/2014 của Bộ trưởng Bộ Y tế về việc ban hành quy định về đảm bảo an toàn thông tin y tế điện tử;

- Cấu hình hệ thống thông tin được chỉ được cài đặt, thay đổi khi được cho phép bằng văn bản của đơn vị;

- Triển khai cách thức lưu lại lịch sử truy cập vào dữ liệu;

- Thực hiện khóa dữ liệu ngay khi phát hiện có truy cập trái phép;

- Thực hiện các biện pháp bảo vệ cơ sở dữ liệu khi triển khai trên mạng nội bộ và Internet theo điều 5, chương II tại quyết định 4159/QĐ-BYT ngày 13/10/2014 của Bộ trưởng Bộ Y tế về việc ban hành quy định về đảm bảo an toàn thông tin y tế điện tử;

- Triển khai hệ thống giám sát truy cập vào hệ thống thông tin để phát hiện các hành vi bất thường khi truy cập, khai thác dữ liệu.

Xin trân trọng cảm ơn!

Nơi nhận:
- Như trên;
- Thứ trưởng Lê Quang Cường (để b/c);
- Cục trưởng (để b/c);
- Lưu: VT, CSHT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ Y TẾ

Lương Chí Thành