BỘ Y TẾ	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 4495 /QĐ-BYT	*Hà Nội, ngày 30 tháng 10 năm 2015*

QUYẾT ĐỊNH

Ban hành Hướng dẫn xây dựng nội quy an toàn, an ninh thông tin trong các đơn vị trong ngành y tế

BỘ TRƯỞNG BỘ Y TẾ

Căn cứ Nghị định số 63/2012/NĐ-CP ngày 31/8/2012 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 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Thông tư số 53/2014/TT-BYT ngày 29/12/2014 của Bộ Y tế quy định điều kiện hoạt động y tế trên môi trường mạng;

Căn cứ Quyết định số 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;

Xét đề nghị của Cục trưởng Cục Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo quyết định này "Hướng dẫn xây dựng nội quy an toàn, an ninh thông tin trong các đơn vị trong ngành y tế".

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

Điều 3. Chánh văn phòng Bộ, Cục trưởng Cục Công nghệ thông tin, Thủ trưởng các đơn vị thuộc/trực thuộc Bộ Y tế và các tổ chức liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng Bộ Y tế (để b/c);
- Các Thứ trưởng Bộ Y tế (để phối hợp chỉ đạo);
- Sở Y tế các tỉnh/thành phố trực thuộc TW;
- Cổng Thông tin điện tử Bộ Y tế;
- Lưu: VT, CNTT (2).

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Lê Quang Cường

BỘ Y TẾ

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

HƯỚNG DẪN

Xây dựng nội quy an toàn, an ninh thông tin trong các đơn vị trong ngành y tế

(Ban hành kèm theo Quyết định số 4495 /QĐ-BYT ngày 30 tháng 10 năm 2015 của Bộ trưởng Bộ Y tế)

I. Phạm vi áp dụng và đối tượng áp dụng

1. Văn bản này hướng dẫn xây dựng các nội dung về nội quy đảm bảo an toàn, an ninh thông tin trong hoạt động y tế trên môi trường mạng tại các đơn vị trong ngành y tế.

2. Hướng dẫn này áp dụng đối với các đơn vị, tổ chức trong ngành y tế khi áp dụng công nghệ thông tin trong hoạt động của đơn vị.

II. Giải thích từ ngữ

1. *Bên thứ ba*: là các tổ chức, cá nhân có chuyên môn được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hóa, dịch vụ công nghệ thông tin.

2. *Tài sản công nghệ thông tin (gọi tắt là tài sản)*: là các trang thiết bị, thông tin, dịch vụ thuộc hệ thống công nghệ thông tin của đơn vị, bao gồm:

a) *Tài sản vật lý*: là các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống công nghệ thông tin;

b) *Tài sản thông tin*: là các dữ liệu, tài liệu liên quan đến hệ thống công nghệ thông tin. Tài sản thông tin được thể hiện bằng văn bản giấy hoặc dữ liệu điện tử;

c) *Tài sản phần mềm*: bao gồm các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển;

d) *Dịch vụ*: là các dịch vụ công nghệ thông tin thuê bên thứ ba cung cấp.

III. Các quy định trong nội quy an toàn, an ninh thông tin

1. Quy định về kiểm soát truy cập vật lý

Quy định này nhằm ngăn cản các truy nhập vật lý không được phép và giảm thiểu thiệt hại đối với các thông tin y tế quan trọng của đơn vị.

a) Những tài sản quan trọng (như máy chủ chạy các ứng dụng quan trọng, các thiết bị lưu trữ thông tin bảo mật) cần được đặt tại các phòng riêng có quy

định chế độ bảo mật cao như khóa, hệ thống xác thực cá nhân và các hệ thống kiểm soát truy cập khác.

b) Quy định những cá nhân nào được phép vào phòng quản lý các tài sản quan trọng và quy định về thủ tục xác thực các cá nhân được phép truy cập, cụ thể như ghi nhận và kiểm tra danh sách truy nhập vào phòng định kỳ.

c) Quy định việc mang vào hoặc đem ra các thiết bị lưu trữ và thiết bị điện tử (ổ đĩa, thiết bị USB, hoặc các sao chép vật lý đối với dữ liệu) đối với các phòng quản lý các tài sản quan trọng nhằm tránh việc lây nhiễm các phần mềm độc hại cho các hệ thống này và tránh rò rỉ các thông tin quan trọng ra ngoài. Xây dựng các thủ tục khai báo và kiểm tra việc mang vào hoặc đem ra đối với các thiết bị trước khi vào hoặc rời phòng.

d) Quy định việc kiểm soát công tác gỡ bỏ các dữ liệu bảo mật và các phần mềm quan trọng khi hủy bỏ hoặc không sử dụng các thiết bị lưu trữ vật lý.

đ) Quy định về môi trường làm việc cho phòng quản lý các thiết bị quan trọng bao gồm nhiệt độ, nguồn điện, phòng cháy chữa cháy.

2. Quy định về quản lý, vận hành hệ thống thông tin

Quy định này đảm bảo tránh việc rò rỉ, mất mát thông tin khi quản lý vận hành hệ thống trang thiết bị công nghệ thông tin và mạng máy tính.

a) Hệ thống máy chủ:

- Quản lý an toàn hệ thống: thủ tục cài đặt, kiểm tra và loại bỏ các dịch vụ không cần thiết trên máy chủ; quy định về các cá nhân được phép truy nhập vào máy chủ; thủ tục đặt và thay đổi mật khẩu đối với hệ thống máy chủ.

- Quản lý tài khoản truy cập: các thủ tục cấp quyền, thay đổi mật khẩu cũng như hủy bỏ quyền truy cập đối với tài khoản truy cập máy chủ.Quy định về việc đặt mật khẩu cho các tài khoản truy cập.

- Cập nhật bản vá lỗ hổng hệ điều hành và phần mềm hệ thống: thủ tục kiểm tra và cập nhật thường xuyên bản vá lỗ hổng hệ điều hành và phần mềm hệ thống.

- Quy định việc cài đặt và cập nhật phiên bản đối với các phần mềm chống vi rút và mã độc.

- Quy định việc sao lưu và phục hồi đối với hệ thống và dữ liệu máy chủ.

b) Truy cập Internet:

- Xây dựng quy định việc kiểm soát truy cập trang web. Có chế độ không cho phép truy cập các trang web không được phép.

- Quy định việc cài đặt phần mềm bảo vệ máy chủ và máy tính cá nhân khi truy cập Internet.

c) Truy cập mạng nội bộ:

- Kiểm soát truy cập mạng LAN: quy định việc cấp quyền truy nhập các dịch vụ, hệ thống của đơn vị trong mạng nội bộ theo nhu cầu công việc của từng nhóm người sử dụng.

- Phân tách vùng mạng: Quy định việc phân tách vùng mạng đối với các nhóm người sử dụng, dịch vụ thông tin, hệ thống thông tin quan trọng, đòi hỏi ưu tiên băng thông cần được quy định một cách hợp lý.

- Có quy định việc kết nối vào mạng không dây nội bộ. Đảm bảo việc truy cập mạng không dây nội bộ chỉ cho phép ở khu vực quy định và sử dụng cho hoạt động của đơn vị. Có quy định kiểm soát các truy cập không được phép vào mạng không dây nội bộ của đơn vị.

- Truy cập mạng nội bộ từ xa: có thủ tục kiểm soát việc xác thực và hoạt động của người sử dụng yêu cầu truy nhập vào mạng nội bộ từ xa.

d) Thư điện tử:

- Xây dựng các quy định về việc sử dụng thư điện tử để tránh việc gửi, nhận hoặc làm mất mát các thông tin quan trọng trong quá trình sử dụng thư điện tử.

- Quy định về lọc thư điện tử để loại bỏ thư rác và các thư chứa nội dung không mong muốn.

đ) Máy tính cá nhân:

- Quản lý an toàn hệ thống: thủ tục cài đặt, kiểm tra và loại bỏ các dịch vụ, phần mềm không cần thiết trên máy tính cá nhân;

- Quản lý quyền truy cập: quy định việc đặt mật khẩu đối với các máy tính cá nhân và màn hình máy tính cá nhân sử dụng trong công việc hàng ngày.

- Quản lý an toàn dữ liệu: quy định việc mã hóa hoặc đặt mật khẩu đối với những dữ liệu, thông tin bảo mật nằm trong máy tính cá nhân.

- Quy định việc cài đặt và cập nhật phiên bản đối với phần mềm chống virus và mã độc.

3. Quy định về quản lý tài sản phần cứng và phần mềm

Quy định việc quản lý tài sản phần cứng và phần mềm nhằm đảm bảo tránh việc rò rỉ hoặc mất mát thông tin trên các thiết bị, ứng dụng quản lý, lưu trữ thông tin.

a) Thủ tục cài đặt, di chuyển hoặc sửa chữa các thiết bị hay phương tiện lưu trữ thông tin quan trọng. Đảm bảo các thao tác trên phải được ghi nhận lại và dữ liệu phải được sao lưu trước khi thực hiện các thao tác trên.

b) Thủ tục cài đặt hay gỡ bỏ các phần mềm quan trọng. Đảm bảo phần mềm được khôi phục khi có sự cố và dữ liệu được sao lưu trước khi thực hiện các thao tác cài đặt hay gỡ bỏ phần mềm.

c) Quy định về tuân thủ các quy trình, hướng dẫn sử dụng phần mềm chuyên ngành của đơn vị. Quy định về trách nhiệm phản hồi khi có phát sinh lỗi, vấn đề bảo mật, các yêu cầu về nghiệp vụ khác liên quan đến phần mềm ứng dụng chuyên ngành tại đơn vị.

4. Quy định về việc quản lý thông tin

Quy định về quản lý thông tin cần được xây dựng để ngăn chặn việc rò rỉ, mất mát các thông tin bảo mật và quy định các thông tin được công bố.

a) Có quy định đối với các thông tin được công bố và cách thức công bố thông tin trên môi trường mạng.

b) Thông tin bảo mật: Là các thông tin quan trọng được bảo mật theo quy định của đơn vị và của Bộ Y tế.

- Có quy định kiểm soát truy cập thông tin bảo mật quy định tại mục 1 và mục 2 của Phần III.

- Các cá nhân tạo ra hoặc chỉnh sửa các thông tin bảo mật đều phải được ghi lại phần mềm hoặc các văn bản, tài liệu.

- Quy định việc phân loại và đăng ký đối với các thông tin bảo mật và xây dựng các thủ tục bảo mật và phân phối nội dung của các thông tin này. Các biện pháp đưa ra đối với các văn bản, tài liệu về các thông tin này đảm bảo việc tránh tiết lộ thông tin khi chưa được phép. Các thông tin được lưu trữ dưới dạng điện tử cần có biện pháp bảo vệ để tránh rò rỉ, mất mát thông tin bởi mã độc, vi rút máy tính hay những cá nhân không có thẩm quyền.

- Các nội dung liên quan hoặc bổ sung của các thông tin bảo mật cũng được bảo vệ giống như đối với các thông tin này. Đảm bảo việc cung cấp các thông tin quan trọng này cho một tổ chức, hay cá nhân đều phải được phê duyệt bởi cấp có thẩm quyền.

- Việc thông báo, truyền đưa đối với các thông tin bảo mật đều phải được phê duyệt bởi cấp có thẩm quyền. Quy định các biện pháp mã hóa hoặc bảo mật các thông tin bảo mật khi thông báo, truyền đưa các thông tin này qua môi trường mạng.

- Quy định về bảo mật thông tin dữ liệu y tế theo phân quyền trong hệ thống thông tin của đơn vị và theo quy định của Bộ Y tế.

5. Quy định về việc quản lý bên thứ ba

Quy định về việc quản lý bên thứ ba cần được xây dựng để ngăn chặn việc rò rỉ hoặc mất mát thông tin quan trọng cho bên thứ ba.

a) Quy định việc truy cập hệ thống đối với bên thứ ba.

b) Quy định công tác giám sát việc đảm bảo an toàn, an ninh thông tin đối với các hoạt động của bên thứ ba.

c) Quy định về việc cam kết của bên thứ ba trong việc truy cập dữ liệu, phần mềm của đơn vị.

d) Quy định về đảm bảo tính toàn vẹn, ổn định của các hàng hóa, dịch vụ mà bên thứ ba cung cấp và đảm bảo không gây ảnh hưởng xấu đến hệ thống công nghệ thông tin hiện có.

6. Quy định về sự chấp hành, đào tạo và nâng cao nhận thức

Mục tiêu của quy định về sự chấp hành, đào tạo và nâng cao nhận thức nhằm nâng cao nhận thức liên quan đến an toàn, bảo mật cho cán bộ, công chức, viên chức trong đơn vị và đảm bảo tính hiệu quả trong việc triển khai nội quy an toàn, bảo mật trong đơn vị.

a) Quy định chế tài và các biện pháp kỷ luật đối với việc vi phạm nội quy bảo mật và truy cập thông tin không được phép.

b) Quy định việc tổ chức đào tạo, nâng cao nhận thức định kỳ về an toàn, bảo mật thông tin và hậu quả trong việc rò rỉ, mất mát thông tin.

c) Quy định về việc đào tạo nâng cao trình độ chuyên môn nghiệp vụ cho các cán bộ chuyên trách an toàn, an ninh thông tin.

IV. Tổ chức thực hiện

Lãnh đạo các đơn vị trong ngành y tế tổ chức xây dựng, triển khai, cập nhật phổ biến nội quy an toàn bảo mật của đơn vị cho cán bộ, công chức, viên chức của đơn vị. Nội dung cơ bản của nội quy bao gồm:

1. Yêu cầu chung

a) Mục tiêu, yêu cầu đối với việc xây dựng nội quy an toàn, bảo mật thông tin của đơn vị.

b) Các khái niệm, tiêu chuẩn, yêu cầu tuân thủ đối với nội quy an toàn, bảo mật thông tin của đơn vị.

2. Yêu cầu cụ thể

a) Phân loại tài sản, thông tin y tế của đơn vị.

b) Áp dụng các hướng dẫn tại phần II của hướng dẫn này để xây dựng nội quy đảm bảo an toàn, an ninh thông tin y tế của đơn vị

c) Các biện pháp kỹ thuật cụ thể đối với từng nội dung hướng dẫn.

d) Các tiêu chuẩn cần đáp ứng đối với từng nội dung hướng dẫn.

3. Tổ chức thực hiện

a) Trách nhiệm của lãnh đạo trong việc ban hành, hướng dẫn, tổ chức thực hiện. Các cam kết hỗ trợ kinh phí, cơ sở vật chất, trang thiết bị kỹ thuật trong việc triển khai nội quy an toàn, bảo mật thông tin của đơn vị.

b) Trách nhiệm của cán bộ kỹ thuật đối với việc xây dựng, cập nhật, kiểm soát việc thi hành nội quy an toàn, bảo mật thông tin của đơn vị.

c) Trách nhiệm của cán bộ, công chức, viên chức của đơn vị trong việc tuân thủ nội quy an toàn, bảo mật thông tin của đơn vị.

d) Quy định về khen thưởng và kỷ luật đối với việc chấp hành nội quy đảm bảo an toàn, an ninh thông tin của đơn vị./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Lê Quang Cường