BỘ Y TẾ	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 4159 /QĐ-BYT	*Hà nội, ngày 13 tháng 10 năm 2014*

QUYẾT ĐỊNH

Ban hành Quy định về đảm bảo an toàn thông tin y tế điện tử tại 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;

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

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo quyết định này "Quy định về đảm bảo an toàn thông tin y tế điện tử tại 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 đơn vị, 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;
- 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

QUY ĐỊNH

Về đảm bảo an toàn thông tin y tế điện tử tại các đơn vị trong ngành y tế

(Ban hành kèm theo Quyết định số 4159 /QĐ-BYT ngày 13 tháng 10 năm 2014 của Bộ trưởng Bộ Y tế)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quyết định này quy định các yêu cầu đảm bảo thông suốt, an toàn, bảo mật thông tin cho việc ứng dụng công nghệ thông tin trong việc quản lý, sử dụng, lưu trữ, truyền đưa các thông tin y tế trên môi trường mạng.

2. Quy định này áp dụng đối với các đơn vị, cơ quan trong ngành y tế triển khai ứng dụng công nghệ thông tin trong quản lý, sử dụng, lưu trữ, truyền đưa thông tin y tế trên môi trường mạng.

Điều 2. Giải thích từ ngữ

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

1. *Thông tin y tế:* bao gồm các thông tin trong các lĩnh vực khác nhau trong ngành y tế.

2. *Thông tin y tế điện tử:* là thông tin y tế được quản lý, sử dụng, lưu trữ, truyền đưa trên môi trường mạng.

3. *Tài khoản đặc quyền:* là tài khoản truy cập vào hệ thống thông tin nhằm thực hiện các công việc đặc biệt hoặc truy cập vào dữ liệu nhạy cảm. Tài khoản đặc quyền thường sử dụng cho việc cấu hình thiết bị, quản trị hệ thống, quản trị hệ điều hành, quản trị cơ sở dữ liệu hay quản trị ứng dụng nghiệp vụ (ví dụ như các tài khoản root, supervisors, system, administrator...).

4. *Bên cung cấp, hỗ trợ:* là những cá nhân, tổ chức cung cấp, hỗ trợ các dịch vụ công nghệ thông tin cho đơn vị bao gồm:

a) Cá nhân, tổ chức cung cấp phần mềm, phần cứng, mạng;

b) Cá nhân, tổ chức bảo trì các dịch vụ cung cấp phần mềm, phần cứng, mạng.

Điều 3. Nguyên tắc chung đối với việc đảm bảo an toàn thông tin y tế

1. *Đảm bảo tính bảo mật*

a) Đảm bảo thông tin y tế chỉ có thể được truy cập bởi những đối tượng (người, chương trình máy tính...) được cấp quyền truy cập.

b) Mật khẩu truy cập, khóa mã hóa và các mã khóa khác được mã hóa trong quá trình truy cập, trên đường truyền và lưu trữ tại đơn vị quản lý thông tin y tế.

2. *Đảm bảo tính toàn vẹn*

a) Đảm bảo tính toàn vẹn thông tin là việc thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi.

b) Việc quản lý, sử dụng, lưu trữ, truyền đưa các thông tin y tế phải đảm bảo tính toàn vẹn, không được thay đổi khi chưa được phép của đơn vị quản lý thông tin y tế.

c) Việc đảm bảo tính toàn vẹn phải được thực hiện trong toàn bộ các quá trình truy cập, các quá trình nhập, lưu trữ, sử dụng, xử lý, truyền tải, trích rút và khôi phục dữ liệu.

3. *Đảm bảo tính sẵn sàng*

a) Đảm bảo khả năng hoạt động liên tục của hệ thống thông tin.

b) Đảm bảo thông tin y tế phải được truy cập nhanh chóng khi có sự yêu cầu từ phía cá nhân, tổ chức được cho phép truy cập thông tin.

c) Đảm bảo nguồn nhân lực trong việc vận hành hệ thống thông tin.

d) Xây dựng, ban hành, tuân thủ các quy trình trong việc quản lý, vận hành hệ thống thông tin.

Chương II

QUY ĐỊNH CỤ THỂ

Điều 4. Ban hành quy định cụ thể về an toàn, bảo mật hệ thống thông tin

1. Các đơn vị cần xây dựng, ban hành quy định cụ thể cho đơn vị về an toàn, bảo mật cho hệ thống thông tin. Quy định cần được phê duyệt bởi lãnh đạo đơn vị, phù hợp với quy định của Nhà nước, ngành y tế và quy chế an toàn, bảo mật của đơn vị. Quy định bao gồm tối thiểu các nội dung sau:

a) Quy định chung (phạm vi, đối tượng, khái niệm, mục đích).

b) Quy định cụ thể (nội dung, tiêu chuẩn, các yêu cầu cần tuân thủ).

c) Trách nhiệm của các bên liên quan.

d) Tổ chức thực hiện.

2. Định kỳ tối thiểu mỗi năm một lần, đơn vị rà soát, chỉnh sửa, hoàn thiện các quy định này đảm bảo sự phù hợp, đầy đủ và hiệu quả của quy định.

Điều 5. Mạng nội bộ và Internet

1. Có biện pháp phát hiện và phòng chống xâm nhập, phòng chống phát tán mã độc hại trên mạng nội bộ và Internet.

2. Có biện pháp phòng chống tấn công từ chối dịch vụ từ bên trong mạng nội bộ và bên ngoài Internet.

3. Yêu cầu có các biện pháp xác thực đảm bảo an toàn đối với các kết nối không dây.

4. Có biện pháp phân tách các phân vùng mạng để đảm bảo kiểm soát được các truy cập hệ thống thông tin và đảm bảo truy cập hiệu quả đối với các dữ liệu cần truy cập nhanh chóng.

5. Xác định, xây dựng và triển khai các phương án dự phòng cho các vị trí có mức độ ảnh hưởng cao tới hoạt động của hệ thống mạng hoặc có khả năng làm tê liệt hệ thống mạng của đơn vị khi xảy ra sự cố.

6. Xác định và đảm bảo nhu cầu băng thông của mạng nội bộ và Internet.

7. Thường xuyên cập nhật các bản vá lỗi hệ thống, cập nhật cấu hình cho các thiết bị mạng và các thiết bị bảo mật.

8. Bảo đảm chất lượng và đầy đủ các trang thiết bị mạng, an ninh, bảo mật, phần mềm chống virus, công cụ phân tích, quản trị mạng được cài đặt trong mạng của đơn vị.

Điều 6. Máy chủ và phần mềm hệ thống

1. Bảo đảm có hạ tầng máy chủ và các thiết bị đi kèm phục vụ hệ thống thông tin đủ công suất, đạt hiệu năng yêu cầu, đảm bảo tốc độ xử lý truy xuất thông tin y tế đáp ứng yêu cầu của đơn vị.

2. Yêu cầu đối với máy chủ:

a) Có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo tính hoạt động liên tục.

b) Máy chủ phải được đặt ở phòng riêng, được bảo vệ an toàn về mặt vật lý. Phòng máy chủ phải được khóa, đặt mã bảo vệ và được giám sát chặt chẽ.

Đảm bảo môi trường cho hoạt động của máy chủ như nguồn điện, nhiệt độ phục vụ cho hoạt động liên tục của máy chủ. Có các biện pháp phòng chống cháy, nổ cho phòng máy chủ. Quy định rõ ràng về quyền hạn, trách nhiệm của những cá nhân được phép vào phòng máy chủ.

3. Việc truy cập máy chủ trực tiếp hoặc từ xa đều phải thông qua kiểm soát bằng mật khẩu hoặc các biện pháp kiểm soát phù hợp khác. Có phương án đặt máy chủ tại các phân vùng mạng phù hợp theo chức năng và yêu cầu bảo mật của máy chủ.

4. Có biện pháp phát hiện, phòng chống xâm nhập, phát tán mã độc hại và virus máy tính cho máy chủ.

5. Yêu cầu đối với phần mềm hệ thống:

a) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế (như UNIX, LINUX và các hệ điều hành thông dụng khác).

b) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

c) Thường xuyên rà soát, cập nhật các phiên bản vá lỗi phần mềm hệ thống.

Điều 7. Máy trạm

1. Máy trạm (bao gồm máy tính để bàn và máy tính xách tay) tối thiểu yêu cầu được bảo vệ bằng mật khẩu.

2. Các cơ sở dữ liệu hoặc các tập tin chứa thông tin y tế quan trọng yêu cầu được bảo vệ bằng mật khẩu.

3. Yêu cầu có phương án phát hiện, phòng chống xâm nhập, phát tán mã độc hại và virus cho máy trạm.

4. Yêu cầu có phương án bảo vệ dữ liệu máy trạm nếu kết nối với mạng Internet.

5. Đối với các máy trạm trực tiếp làm việc với người dân tại các cơ sở y tế, cần đảm bảo thông tin y tế trên màn hình máy tính trong lúc làm việc không được xem bởi các cá nhân không được phép. Đặt chế độ khóa màn hình khi không làm việc trên máy tính.

6. Thường xuyên cập nhật bản vá lỗi và nâng cấp hệ điều hành.

Điều 8. Phần mềm ứng dụng

1. Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận

hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật.

2. Yêu cầu có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng.

3. Yêu cầu tiến hành kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị.

4. Quản lý chặt chẽ các tài khoản phát sinh trước, trong và sau khi triển khai phần mềm ứng dụng.

5. Quản lý và nâng cấp phiên bản

a) Yêu cầu đánh giá hiệu quả, ảnh hưởng khi tích hợp với các phần mềm khác, rủi ro gặp phải khi nâng cấp phiên bản.

b) Các phiên bản nâng cấp cần được thử nghiệm tính an toàn, bảo mật, báo cáo lãnh đạo phê duyệt trước khi đưa vào sử dụng.

c) Yêu cầu có phương án phục hồi lại phần mềm khi không nâng cấp được phiên bản mới.

d) Yêu cầu ghi lại quá trình nâng cấp phần mềm bao gồm lý do, phiên bản, thời gian, người nâng cấp.

e) Các phiên bản phần mềm cần được quản lý chặt chẽ và lưu tại vị trí được bảo mật.

g) Yêu cầu có tài liệu hướng dẫn nâng cấp, sử dụng, cài đặt chi tiết khi tiến hành nâng cấp phiên bản phần mềm.

6. Kiểm soát chương trình nguồn

a) Chỉ định cụ thể các cá nhân quản lý chương trình nguồn của phần mềm ứng dụng.

b) Việc truy cập tới chương trình nguồn phải được sự phê chuẩn của cấp có thẩm quyền và được ghi lại.

c) Chương trình nguồn phải được lưu trữ an toàn tại ít nhất hai địa điểm tách biệt.

d) Phải có cam kết không chứa mã độc hại giữa bên cung cấp, hỗ trợ và đơn vị khi triển khai phần mềm ứng dụng.

7. Khuyến khích việc tăng cường sử dụng các phần mềm bản quyền, hạn chế tối đa việc sử dụng phần mềm không hợp pháp. Đơn vị, cá nhân chịu trách nhiệm về các hậu quả phát sinh do việc sử dụng các phần mềm không hợp pháp.

Điều 9. Thư điện tử

1. Không sử dụng các hộp thư điện tử công cộng, không được xác thực và không đảm bảo tính an toàn, bảo mật thông tin cho các mục đích trao đổi công việc của đơn vị. Không sử dụng thư điện tử chính thức của đơn vị vào mục đích cá nhân.

2. Khuyến khích việc đặt mật khẩu và sử dụng các định dạng không chỉnh sửa được cho các tập tin quan trọng đính kèm thư điện tử.

3. Bảo đảm mỗi hộp thư điện tử cá nhân chỉ được truy cập bởi cá nhân đó. Mỗi cá nhân cần đặt mật khẩu đủ mạnh cho hộp thư điện tử của mình. Chỉ có cá nhân quản lý hộp thư điện tử mới được quyền thay đổi mật khẩu hộp thư điện tử của mình.

4. Đơn vị quản lý hệ thống thư điện tử cần có quy định về việc khóa và xóa bỏ hộp thư điện tử cá nhân khi cá nhân đó không còn làm việc tại đơn vị.

5. Đơn vị quản lý hệ thống thư điện tử cần xây dựng phương án đảm bảo an toàn và tính sẵn sàng truy cập cho hệ thống thư điện tử trong nội bộ và trên Internet, phương án chống thư rác cho thư điện tử.

Điều 10. Cơ sở dữ liệu

1. Chỉ được sử dụng hệ quản trị cơ sở dữ liệu có bản quyền, nguồn gốc, xuất xứ rõ ràng, hoặc các hệ quản trị cơ sở dữ liệu mã nguồn mở nhưng được sử dụng rộng rãi trong nước và quốc tế (như MySQL, PostgreSQL, MongoDB hoặc các hệ quản trị cơ sở dữ liệu thông dụng khác).

2. Hệ quản trị cơ sở dữ liệu sử dụng cho hệ thống thông tin của đơn vị cần đáp ứng được yêu cầu hoạt động ổn định; xử lý, lưu trữ được khối lượng dữ liệu của đơn vị theo yêu cầu nghiệp vụ; có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu.

3. Thường xuyên rà soát, cập nhật các bản vá, các bản sửa lỗi hệ quản trị cơ sở dữ liệu.

4. Xây dựng phương án sao lưu, dự phòng đối với cơ sở dữ liệu, đảm bảo khôi phục dữ liệu nhanh chóng khi có sự cố xảy ra. Việc sao lưu dữ liệu được quy định tại Điều 11 của quy định này.

5. Thực hiện phân quyền và có quy định chặt chẽ với từng cá nhân truy cập đến cơ sở dữ liệu, khuyến khích việc ghi nhật ký đối với các truy cập và các thao

tác cơ sở dữ liệu nhưng phải không ảnh hưởng đến tốc độ xử lý dữ liệu của cơ sở dữ liệu.

6. Yêu cầu có các phương án ngăn chặn các hình thức tấn công và truy cập cơ sở dữ liệu trái phép.

Điều 11. Sao lưu, phục hồi

1. Đối với dữ liệu trên máy tính cá nhân:

a) Đối với các dữ liệu quan trọng, sao lưu cần được thực hiện khi dữ liệu có sự thay đổi. Đảm bảo các dữ liệu quan trọng được phục hồi nguyên vẹn khi cần thiết.

b) Đảm bảo dữ liệu cần thiết trên máy tính đều được sao lưu khi có các thay đổi hoặc nâng cấp bất kỳ đối với hệ điều hành.

c) Phương tiện sao lưu và quy trình phục hồi phải được kiểm tra thường xuyên nếu có thể để đảm bảo sẵn sàng sử dụng cho trường hợp khẩn cấp.

d) Dữ liệu sao lưu phải được lưu ở vị trí an toàn, cách xa dữ liệu gốc và những người không được cho phép. Đối với những dữ liệu quan trọng, khuyến khích dữ liệu sao lưu đặt cách xa vị trí địa lý của đơn vị.

2. Đối với cơ sở dữ liệu trên máy chủ:

a) Các dữ liệu sao lưu và các bản sao lưu hoàn chỉnh của cơ sở dữ liệu và tài liệu quy trình phục hồi phải được lưu trữ ở các địa điểm cách xa vị trí cài đặt để đảm bảo tránh khỏi các sự cố nghiêm trọng nếu có. Số bản sao lưu phải được đơn vị tính toán để đảm bảo phục hồi dữ liệu theo yêu cầu của đơn vị, đặc biệt đối với các dữ liệu quan trọng.

b) Phương tiện sao lưu phải được kiểm tra thường xuyên để sẵn sàng sử dụng trong trường hợp khẩn cấp.

c) Dữ liệu sao lưu cần được lưu giữ tại một địa điểm được bảo vệ vật lý và có môi trường đồng bộ với các tiêu chuẩn áp dụng tại địa điểm chính.

d) Cần xác định thời gian lưu trữ cho các thông tin quan trọng và các yêu cầu cho các bản sao lưu trữ vĩnh viễn.

e) Quy trình phục hồi cơ sở dữ liệu phải được kiểm tra thường xuyên để đảm bảo hiệu quả và có thể hoàn thành trong thời gian cho phép.

3. Đối với phần mềm:

Bản gốc phần mềm đã mua phải được lưu trữ an toàn để có thể cài lại nhanh chóng trong trường hợp máy tính hỏng.

Điều 12. Trao đổi thông tin y tế trên môi trường mạng

1. Sử dụng các phương pháp định danh phù hợp với quy định của Pháp luật và Bộ Y tế.

2. Sử dụng các phương pháp mã hóa phù hợp đáp ứng yêu cầu bảo mật và khả năng xử lý của hệ thống thông tin để bảo mật thông tin y tế điện tử và tính toàn vẹn của thông tin.

3. Các khóa mã hóa phải được khởi tạo, thay đổi, phân phối, lưu trữ một cách an toàn.

4. Đảm bảo khôi phục được các thông tin đã mã hóa khi cần thiết.

5. Xây dựng quy định về thu hồi, hủy khóa và phục hồi khóa mã hóa.

Điều 13. Tài khoản người sử dụng

1. Xây dựng quy trình chính thức bằng văn bản để quy định quyền truy cập vào mạng, máy chủ, phần mềm ứng dụng, cơ sở dữ liệu của từng cán bộ trong đơn vị. Các quy trình này bao gồm tất cả các quy định đối với cán bộ, bao gồm từ lúc đăng ký truy cập tới khi hủy bỏ đăng ký truy cập.

2. Cần có quy định kiểm soát và theo dõi chặt chẽ việc truy cập vào các tài khoản đặc quyền.

3. Các quy tắc bảo mật cơ bản đối với tài khoản người sử dụng bao gồm:

a) Chỉ cho phép mỗi người sử dụng có một tài khoản truy cập.

b) Áp dụng quy tắc phân quyền tài khoản người sử dụng theo quyền của nhóm tài khoản.

c) Yêu cầu mật khẩu được thay đổi một cách thường xuyên (ít nhất là mỗi tháng một lần).

d) Các đơn vị cần có quy định về mật khẩu mạnh (như quy định số ký tự tối thiểu của mật khẩu, bắt buộc có cả chữ in hoa, chữ thường hay bắt buộc có cả ký tự chữ và số).

e) Khi một người dùng mới được quyền truy cập vào hệ thống thông tin, đảm bảo rằng họ được cấp mật khẩu tạm thời. Sau lần truy cập đầu, người sử dụng cần thay đổi mật khẩu tạm thời này. Nếu hệ thống thông tin cho phép, yêu cầu không sử dụng lại mật khẩu cũ.

g) Có quy trình để loại bỏ ngay lập tức các tài khoản và quyền truy cập hệ thống của người thay đổi công việc, hoặc không còn làm việc tại đơn vị.

Điều 14. Truy cập từ xa

1. Xác thực người dùng và nhận dạng: chủ động xác định được ai đang sử dụng hệ thống thông tin và xác định mức độ truy cập được yêu cầu. Việc nhận dạng tối thiểu bằng mật khẩu. Đối với các tài nguyên quan trọng, cần xem xét sử dụng thẻ thông minh, sinh mã ngẫu nghiên (Token key) hoặc sinh trắc học.

2. Bảo vệ các dữ liệu đang truyền đưa: nếu dữ liệu là bí mật cần sử dụng các công nghệ mã hóa phù hợp.

3. Bảo vệ tài nguyên mạng: có phương án kiểm soát các tài nguyên được yêu cầu truy cập từ xa.

Điều 15. Hủy bỏ các thiết bị lưu trữ thông tin y tế

1. Các thiết bị có chứa thông tin y tế quan trọng như ổ cứng, băng đĩa cần được kiểm tra và đảm bảo rằng bất kỳ dữ liệu và phần mềm cấp phép nào phải được gỡ bỏ hay định dạng lại trước khi hủy bỏ.

2. Thiết bị lưu trữ thông tin y tế quan trọng hư hỏng không còn hoạt động phải được phá hủy vật lý trước khi hủy bỏ.

Điều 16. Đảm bảo tính liên tục của hệ thống thông tin

1. Xây dựng, ban hành phương án đảm bảo tính liên tục của hệ thống thông tin.

2. Có phương án sao lưu, phục hồi dữ liệu theo quy định tại Điều 11 của Quyết định này.

3. Đảm bảo việc truy cập dữ liệu nhanh chóng, không gián đoạn.

4. Có phương án đảm bảo dự phòng hệ thống mạng theo quy định tại Điều 5 của Quy định này.

5. Có phương án đảm bảo tính liên tục của hệ thống máy chủ. Khuyến khích sử dụng các công nghệ đảm bảo tính sẵn sàng cho hệ thống máy chủ.

Điều 17. Quản lý sự cố

1. Xây dựng quy trình quản lý sự cố trong hoạt động công nghệ thông tin của đơn vị mình. Quy trình quản lý sự cố phải được rà soát, cập nhật sự cố và các phương án xử lý tối thiểu sáu tháng một lần.

2. Áp dụng các giải pháp kỹ thuật để phát hiện, xử lý kịp thời các cuộc tấn công từ chối dịch vụ như sử dụng thiết bị tường lửa; thiết bị phát hiện và ngăn chặn xâm nhập; các thiết bị chuyên dụng cảnh báo tấn công, làm lệch hướng lưu lượng mạng; lọc gói tin khi bị tấn công.

3. Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

Điều 18. Bố trí nhân sự

1. Mỗi đơn vị cần bố trí tối thiểu một cán bộ có chuyên môn phù hợp làm đầu mối theo dõi công tác đảm bảo an toàn, bảo mật thông tin y tế điện tử tại đơn vị.

2. Các nhiệm vụ quản trị hệ thống; phát triển, bảo trì phần mềm ứng dụng và vận hành hệ thống cần được phân công cho từng bộ phận, cá nhân cụ thể. Đảm bảo không có cá nhân nào có thể có toàn quyền trên hệ thống trừ cá nhân được lãnh đạo đơn vị cho phép. Ban hành quy định bằng văn bản về trách nhiệm và phân quyền rõ ràng cho từng nhóm bộ phận, cá nhân nêu trên.

3. Yêu cầu có phương án quản lý chặt chẽ việc truy cập hệ thống thông qua tài khoản đặc quyền.

4. Tổ chức đào tạo, nâng cao chuyên môn nghiệp vụ cho các cán bộ làm công tác an toàn thông tin tại đơn vị.

5. Phổ biến quy định về an toàn thông tin cho các cán bộ khi được tuyển dụng vào đơn vị.

Điều 19. Giám sát bên cung cấp, hỗ trợ

1. Có quy định cụ thể, rõ ràng và thực hiện đầy đủ công tác quản lý, giám sát nhân sự bên cung cấp, hỗ trợ khi truy cập vào hệ thống.

2. Có quy định cụ thể bằng văn bản và được lãnh đạo đơn vị chấp thuận về phương án đảm bảo an toàn, bảo mật thông tin khi có bên cung cấp, hỗ trợ truy cập trực tiếp hay gián tiếp vào hệ thống.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 20. Trách nhiệm thi hành

1. Cục Công nghệ thông tin có trách nhiệm hướng dẫn, theo dõi, kiểm tra việc thi hành Quy định này của các đơn vị thuộc ngành y tế. Hàng năm thông qua báo cáo của các đơn vị hoặc thực hiện kiểm tra tại chỗ để đánh giá việc tuân thủ quy định và đảm bảo an toàn, bảo mật cho hệ thống của các đơn vị; tổng hợp, báo cáo lãnh đạo Bộ tình hình về an toàn, bảo mật hệ thống của các đơn vị trong ngành y tế.

2. Hàng năm Cục Công nghệ thông tin – Bộ Y tế có trách nhiệm tổ chức các lớp đào tạo, cập nhật bổ sung về công tác đảm bảo an toàn thông tin y tế cho các đơn vị.

Điều 21. Yêu cầu báo cáo

1. Sở y tế và các đơn vị trực thuộc Bộ Y tế có trách nhiệm gửi báo cáo hàng năm theo mẫu tại Phụ lục I về tình hình đảm bảo an toàn thông tin y tế điện tử tại đơn vị mình và các đơn vị trực thuộc trước ngày 31 tháng 03 hàng năm; hoặc báo cáo đột xuất theo yêu cầu của Bộ Y tế.

2. Các báo cáo theo yêu cầu của khoản 1 điều này được gửi về Cục Công nghệ thông tin – Bộ Y tế.

KT.BỘ TRƯỞNG
THỨ TRƯỞNG

Lê Quang Cường

PHỤ LỤC I

BIỂU MẪU BÁO CÁO TÌNH HÌNH ĐẢM BẢO AN TOÀN THÔNG TIN Y TẾ ĐIỆN TỬ

(Ban hành kèm theo Quyết định số /QĐ-BYT ngày tháng năm 2014 của Bộ trưởng Bộ Y tế)

MỤC 1. THÔNG TIN CHUNG

1. Năm báo cáo: .....

2. Tên cơ quan báo cáo: .....

3. Địa chỉ: .....

4. Điện thoại: ..... Fax: .....

5. Thư điện tử liên hệ: .....

6. Địa chỉ trang/cổng thông tin điện tử (Website/Portal) chính thức: .....

MỤC 2. THÔNG TIN LIÊN HỆ

1. Họ và tên người thực hiện báo cáo: .....

2. Đơn vị công tác: .....

3. Chức vụ: .....

4. Điện thoại cố định: ..... Điện thoại di động: .....

5. Thư điện tử: .....

MỤC 3. TÌNH HÌNH ĐẢM BẢO AN TOÀN THÔNG TIN TẠI ĐƠN VỊ

1. Các hệ thống, phần mềm ứng dụng của đơn vị hiện đang sử dụng

2. Các nội dung đảm bảo an toàn thông tin theo quy định này

a) Ban hành (hoặc chỉnh sửa) quyết định đảm bảo an toàn hệ thống thông tin tại đơn vị

b) Mạng nội bộ và Internet

c) Máy chủ và phần mềm hệ thống

d) Máy trạm

e) Phần mềm ứng dụng

g) Thư điện tử

h) Cơ sở dữ liệu

i) Sao lưu, phục hồi

k) Trao đổi thông tin y tế trên môi trường mạng

l) Tài khoản người sử dụng

m) Truy cập từ xa

n) Hủy bỏ các thiết bị lưu trữ thông tin y tế

o) Đảm bảo tính liên tục của hệ thống

p) Quản lý sự cố

q) Tổ chức thực hiện

3. Những sự cố phát sinh trong năm và phương án khắc phục

4. Kiến nghị, đề xuất

....., ngày ..... tháng ..... năm	....., ngày ..... tháng ..... năm .....
Người lập báo cáo	**Thủ trưởng cơ quan**
(Ký và ghi rõ họ, tên)	*(Ký tên, đóng dấu)*