UBND TỈNH THÁI BÌNH
SỞ Y TẾ

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

Số: 433 /QĐ-SYT

Thái Bình, ngày 28 tháng 8 năm 2017

QUYẾT ĐỊNH
Ban hành Quy định đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Y tế và các đơn vị trực thuộc năm 2017

GIÁM ĐỐC SỞ Y TẾ THÁI BÌNH

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006; Luật An toàn thông tin mạng ngày 19/11/2015;

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

Căn cứ Quyết định 1874/QĐ-UBND ngày 13/7/2017 của UBND tỉnh Thái Bình ban hành Quy định đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị trên địa bàn tỉnh

Quyết định số 997/QĐ-UBND ngày 12/5/2009 của UBND tỉnh Thái Bình về chức năng, nhiệm vụ, quyền hạn và tổ chức bộ máy của Sở Y tế;

Xét đề nghị của Trưởng phòng Kế hoạch tài chính,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Y tế.

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

Điều 3. Chánh văn phòng, chánh thanh tra, trưởng các phòng, ban thuộc Sở Y tế, Giám đốc các đơn vị trực thuộc, công chức, viên chức Sở Y tế, các tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- GĐ, PGĐ Sở;
- Các đơn vị trực thuộc;
- Các phòng, ban thuộc Sở;
- Lưu: VT, KHTC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ Y TẾ
TỈNH THÁI BÌNH

Trần Quang Hải

UBND TỈNH THÁI BÌNH
SỞ Y TẾ

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

QUY ĐỊNH
Về việc Quy định đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Y tế

(Kèm theo Quyết định số 433 /QĐ-SYT ngày 28 tháng 8 năm2017 của Giám đốc Sở Y tế)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Phạm vi áp dụng:

Quy định này bao gồm các nội dung về công tác đảm bảo an toàn thông tin mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp hệ thông thông tin của cơ quan, đơn vị trực thuộc Sở Y tế.

2. Đối tượng áp dụng:

a) Các phòng, ban, đơn vị thuộc Sở Y tế

a) Cán bộ, công chức, viên chức, nhân viên đang công tác tại các đơn vị nêu tại khoản a mục này và những cá nhân, tổ chức có lieenquan áp dụng quy định này trong việc vận hành, khai thác các hệ thống công nghệ thông tin, dùng chung của tỉnh và các hệ thống thông tin tại Sở Y tế và các đơn vị trực thuộc

Điều 2. Giải thích từ ngữ

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

1. Hệ thống thông tin dùng chung của tỉnh, hệ thống thông tin tại các cơ quan, đơn vị là tập hợp các thiết bị viễn thông, công nghệ thông tin bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin số tại Trung tâm tích hợp dữ liệu của tỉnh, tại các cơ quan, đơn vị

2. An toàn thông tin mạng là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm đảm bảo tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

3. Thiết bị di động thông minh được hiểu là thiết bị di động tích hợp một nền tảng hệ điều hành di động với nhiều tính năng hỗ trợ tiên tiến về điện toán và kết nối dựa trên nền tảng cơ bản của thiết bị di động thông thường.

Điều 3. Các hành vi bị nghiêm cấm

1. Tạo ra, cài đặt, phát tán virus máy tính, phần mềm độc hại trái pháp luật.

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 4. Các quy định chung về đảm bảo an toàn thông tin

1. Các văn bản có nội dung mật không được truyền trên mạng mà phải được quản lý theo chế độ mật theo quy định pháp luật hiện hành. Không sử dụng các thiết bị di động thông minh để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định. Trường hợp đặc biệt, cần truyền thông tin mật trên mạng phải được Thủ trưởng cơ quan, đơn vị cho phép, trước khi truyền thông tin phải được mã hóa theo quy định của Luật cơ yếu. Các thiết bị viễn thông, máy tính được sử dụng để lưu trữ và truyền thông bí mật nhà nước phải được chứng nhận của cơ quan chức năng kiểm tra, kiểm định trước khi đưa vào sử dụng.

2. Đối với Sở Y tế và các cá nhân tham gia khai thác mạng văn phòng điện tử liên thông: trao đổi văn bản, tài liệu điện tử chỉ thực hiện trên hệ thống thông tin dùng chung của tỉnh và hệ thống thông tin của cơ quan. Không trao đổi văn bản tài liệu điện tử qua mạng xã hội, qua thư điện tử công cộng (gmail, yahoo mail,...), không sử dụng dịch vụ lưu trữ trực tuyến (Google drive, dropbox,...) để lưu trữ, chia sẻ văn bản, tài liệu của cơ quan.

3. Các cơ quan, đơn vị phải sử dụng phần mềm diệt virus có bản quyền cho 100% máy tính của phòng ban, đơn vị khi kết nối mạng nội bộ, mạng diện rộng của tỉnh, hệ thống phần mềm của đơn vị.

4. Phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của phòng ban, đơn vị. Lãnh đạo phòng ban, đơn vị phải chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

5. Để phục vụ hoạt động theo dõi, giám sát, phân tích và điều tra, các cơ quan, đơn vị quản trị hệ thống công nghệ thông tin phải thực hiện lưu trữ nhật

ký của các hệ thông công nghệ thông tin tại các máy chủ(của HĐH và các phần mềm ứng dụng) trong thời gian ít nhất là 30 ngày.

6. Các thiết bị viễn thông, máy tính chứa tài liệu của cơ quan nhà nước khi đưa đi công tác nước ngoài phải thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước.

7. Chú trọng phát triển nguồn nhân lực có trình độ về công nghệ thông tin đặc biệt là an toàn thông tin để nâng cao năng lực bảo đảm an toàn thông tin. Tạo điều kiện cho cán bộ phụ trách công nghệ thông tin được đào tạo, bồi dưỡng nâng cao nghiệp vụ về an toàn thông tin.

Điều 5. Đảm bảo an toàn thông tin cho các hệ thống thông tin và các thiết bị công nghệ thông tin

1. Nội dung bảo vệ hệ thống thông tin được thực hiện theo các quy định tại Điều 22,23 của Luật an toàn thông tin mạng; Điều 19,20,22 của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

Khi xây dựng, nâng cấp, mở rộng hạ tầng kỹ thuật công nghệ thông tin; các hệ thống thông tin của cơ quan, đơn vị phải có phương án đảm bảo an toàn thông tin mạng và phải được Sở Thông tin và Truyền thông thẩm định trước khi cấp có thẩm quyền phê duyệt.

- Việc quản lý, gửi thông tin trên mạng phải tuân thủ theo các nội dung quy định tại Điều 10, Luật an toàn thông tin mạng và các quy định sau:

- Việc trao đổi văn bản, tài liệu điện tử của phòng ban, đơn vị (kể cả tài liệu tham khảo) chỉ thực hiện trên các hệ thống ứng dụng công nghệ thông tin dùng chung của tỉnh hoặc trên các phần mềm ứng dụng của nội bộ ngành chuyển giao ứng dụng.

- Khi phát hành và gửi văn bản qua mạng, các đơn vị phải thực hiện ký số và xác thực văn bản điện tử trước khi gửi.

- Máy chủ, máy tính cá nhân và hệ thống lưu trữ nội bộ, thiết bị mạng phải được bảo vệ bởi mật khẩu an toàn, tuyệt đối không sử dụng mật khẩu ngắn, mặc định; thực hiện việc bảo vệ an toàn vật lý cho hệ thống thông tin của cơ quan, đơn vị;

- 100% máy tính của các phòng ban, đơn vị phải được cài đặt phần mềm diệt virus có bản quyền. Khi phát hiện hoặc có thông tin trong hệ thống mạng bị lây nhiễm các phần mềm gián điệp, độc hại phải khẩn trương và kiên quyết khác phụ sớm và báo cáo tình hình mất an toàn thông tin mạng thông qua đường dây nóng của Sở Y tế.

- Phối hợp xây dựng phương án, tổ chức khắc phục khi xảy ra sự cố an toàn thông tin mạng.

2. Đảm bảo an toàn thông tin cho trung tâm tích hợp dữ liệu của tỉnh:

- Các đơn vị đặt dữ liệu hoặc kết nối vào Trung tâm tích hợp dữ liệu của tỉnh phải tuân thủ các chính sách an toàn thông tin liên quan đến việc kết nối vào Trung tâm tích hợp dữ liệu của tỉnh do Sở Thông tin và truyền thông hướng dẫn

- Các đơn vị khi kết nối vào Trung tâm tích hợp dữ liệu của tỉnh phải tự bảo vệ hệ thống đầu cuối của mình và phải chịu trách nhiệm nếu để tin tặc kiểm soát máy tính và tấn công ngược vào Trung tâm tích hợp dữ liệu của tỉnh.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 6. Trách nhiệm chung các các phòng ban, đơn vị

1. Các đơn vị nếu triển khai các hệ thống thông tin độc lập thì phải tuân thủ các quy định tại Điều 5 của quy định này đồng thời tự chịu trách nhiệm đảm bảo an toàn thông tin như: Cập nhật kịp thời các bản vá lỗ hổng bảo mật từ nhà cung cấp, nhà sản xuất cho các hệ thống thông tin, cơ sở dữ liệu; có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn để sẵn sàng phục hồi cơ sở dữ liệu khi xảy ra sự cố an toàn thông tin mạng; tổ chức phân quyền truy cập cho các đối tượng người dùng tham gia vận hành, khai thác các hệ thống thông tin đúng quy trình, chặt chẽ gắn với trách nhiệm của từng tổ chức, cá nhân để đảm bảo an toàn thông tin mạng cho các hệ thống thông tin cơ quan, đơn vị đang quản lý, vận hành và phối hợp với Sở Y tế khi được yêu cầu.

2. Thủ trưởng các cơ quan, đơn vị có trách nhiệm bố trí cán bộ chuyên trách công nghệ thông tin; giao nhiệm vụ giám sát an toàn hệ thống thông tin của cơ quan, quản lý chặt chẽ các tài khoản đã được cung cấp cho người sử dùng trong cơ quan, đơn vị. Cán bộ chuyên trách được đảm bảo điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ. Đảm bảo tuyệt đối an toàn không để tê liệt hệ thống cho hệ thống thông tin khám chữa bệnh tại các đơn vị.

3. Tuyên truyền, nâng cao nhận thức cho cán bộ, công chức, viên chức về các nguy cơ mất an toàn của hệ thống thông tin; tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Giám đốc Sở trong công tác đảm bảo an toàn thông tin của cơ quan, đơn vị mình.

4. Trang bị đầy đủ kiến thức bảo mật cơ bản cho cán bộ, công chức viên chức về an toàn thông tin trước khi cho phép truy nhập và sử dụng hệ thống thông tin.

5. Triệt để sử dụng chứng thư số chuyên dùng ký số và xác thực văn bản điện tử để đảm bảo xác định nguồn góc, tính toàn vẹn của văn bản và mã hóa các tài liệu quan trọng.

6. Phân công cán bộ giám sát, theo dõi thường xuyên hoạt động của cổng thông tin điện tử cơ quan để phát hiện kịp thời và có giải pháp xử lý khi bị thay đổi thông tin, bị đăng tải những thông tin lạ.

7. Quan tâm và ưu tiên bố trí kinh phí cho việc mua sắm, nâng cấp các trang thiết bị phần cứng, phần mềm bảo mật để đảm bảo và tăng cường an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan, đơn vị. Duy trì thường xuyên công tác kiểm tra, đánh giá an toàn thông tin đối với hệ thống thông tin của đơn vị.

8, Khi có sự cố hoặc có nguy cơ mất an toàn thông tin phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị, báo cáo cho doanh nghiệp cung cấp dịch vụ và thông báo bằng văn bản cho Sở Y tế biết. Trường hợp không khắc phục được thì phối hợp cùng Sở Y tế, Sở Thông tin và truyền thông hoặc cơ quan cấp trên để được hướng dẫn, hỗ trợ.

9. Xây dựng quy định, quy trình nội bộ về đảm bao an toàn thông tin trong khai thác, sử dụng các hệ thống thông tin của cơ quan, đơn vị phù hợp với Quy định này và các quy định khác của pháp luật.

10. Khi triển khai đầu tư ứng dụng công nghệ thông tin phải có phương án đảm bảo an toàn thông tin từ khâu thiết kế và phải tự chịu trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin của cơ quan, đơn vị mình.

11. Phối hợp chặt chẽ với Công an tỉnh trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

12. Phối hợp với Sở Y tế và các đơn vị liên quan thực hiện công tác kiểm tra khắc phục sự cố đồng thời cung cấp đầy đủ các thông tin khi đoàn kiểm tra yêu cầu. Không được che dấu thông tin về sự cố nhằm gây khó khăn cho các cơ quan chức năng đánh giá thiệt hại có phương án xử lý.

13. Định kỳ hàng quý, các đơn vị lập báo cáo về an toàn thông tin gửi về Sở Y tế tổng hợp báo cáo UBND tỉnh theo hướng dẫn tại Điều 16 của Quyết định 1874/QĐ-UBND ngày 13/7/2017 của UBND tỉnh Thái Bình ban hành Quy định đảm bảo an toàn thông tin của các cơ quan, đơn vị trên địa bàn tỉnh.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 7. Trách nhiệm của các đơn vị

1. Phòng Kế hoạch tài chính:

a) Tổ chức phổ biến và triển khai thực hiện quy định này tại cơ quan Sở Y tế và các đơn vị có kết nối vào mạng nội bộ cơ quan Sở Y tế.

b) Trình Lãnh đạo Sở Y tế phê duyệt và tổ chức triển khai kế hoạch ứng phó trong tình huống khẩn cấp (phát hiện có tấn công đánh cắp bí mật nhà nước của ngành Y tế qua đường mạng, các hệ thống quan trọng của ngành Y tế bị chiếm quyền điều khiển).

c) Hướng dẫn, kiểm tra việc thực hiện quy định này của các phòng ban thuộc Sở Y tế, các đơn vị có kết nối trao đổi thông tin với mạng nội bộ cơ quan Sở Y tế.

đ) Tổng hợp, báo cáo Sở Y tế theo định kỳ hàng quý về công tác đảm bảo an toàn thông tin của toàn ngành Y tế theo nội dung của quy định này và các vấn đề về an toàn thông tin phát sinh trong kỳ báo cáo.

e) Trình Sở sửa đổi, bổ sung quy định này để phù hợp với tình hình và điều kiện thực tế.

2. Các đơn vị trực thuộc

a) Phối hợp với Phòng Kế hoạch tài chính – Sở Y tếtrong việc triển khai, thực hiện quy định áp dụng cho đối tượng người dùng tại đơn vị.

b) Phối hợp với Sở Y tế triển khai kế hoạch ứng phó tấn công khẩn cấp về các nội dung liên quan tới đơn vị.

c) Phản ánh nhu cầu, vướng mắc trong quá trình triển khai, thực hiện đảm bảo an ninh thông tin tại đơn vị tới phòng Kế hoạch tài chính.

3. Cơ quan, tổ chức, cá nhân ngoài ngành Y tế có liên quan:

a) Tuân thủ quy định này, quy định công tác bảo vệ bí mật nhà nước của ngành Y tế, các cam kết, đảm bảo an toàn thông tin khi cung cấp dịch vụ công nghệ thông tin và thực hiện các hoạt động trao đổi thông tin với các phòng ban thuộc Sở Y tế. Trường hợp tham gia sử dụng ứng dụng của ngành Y tế, phải tuân thủ các yêu cầu, hướng dẫn, quy trình đảm bảo an toàn thông tin cụ thể của ứng dụng.

b) Phản ánh vướng mắc, nguy cơ, rủi ro ảnh hưởng đến an toàn thông tin của ngành Y tế phát hiện được trong quá trình làm việc đề nghị phản ánh về Sở Y tế để cùng phối hợp xử lý, giải quyết.

Điều 8. Các điều khoản thi hành

1. Các cơ quan, đơn vị, tổ chức cá nhân có hành vi vi phạm Quy định này tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật.

2. Trong quá trình thực hiện, nếu có vướng mắc, phát sinh hoặc các vấn đề cần bổ sung đề nghị các đơn vị kịp thời phản ánh về Sở Y tế để tổng hợp, xem xét, quyết định./.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ Y TẾ TỈNH THÁI BÌNH

Trần Quang Hải