

QUY ĐỊNH

Về việc đảm bảo an toàn, an ninh thông tin về bí mật nhà nước trong lĩnh vực thông tin số tại Trung tâm Y tế huyện Hòa Vang

Căn cứ Pháp lệnh bảo vệ bí mật nhà nước ngày 28 tháng 12 năm 2000;

Căn cứ Nghị định số 33/2002/NĐ-CP ngày 28 tháng 3 năm 2002 của Chính phủ quy định chi tiết thi hành Pháp lệnh bảo vệ bí mật nhà nước;

Căn cứ Thông tư Số: 06/2015/TT-BYT ngày 31 tháng 3 năm 2015 của Bộ Y tế Quy định công tác bảo vệ bí mật nhà nước trong ngành Y tế;

Căn cứ Quyết định số 7562/QĐ-BYT ngày 29 tháng 12 năm 2016 của Bộ trưởng Bộ Y tế về việc Ban hành 05 Bộ chỉ số đánh giá mức độ sáng sủa về ứng dụng công nghệ thông tin trong ngành y tế;

I./ NHỮNG QUY ĐỊNH CHUNG

1. Phạm vi áp dụng

Quy định về công tác bảo vệ bí mật nhà nước tại Trung tâm Y tế huyện Hòa Vang từ khâu soạn thảo, in, sao, chụp, gửi, nhận, thu hồi, lưu giữ, thống kê, sử dụng, bảo quản, tiêu hủy tài liệu, vật mang bí mật nhà nước trên toàn trung tâm.

2. Đối tượng áp dụng

Quy định này áp dụng đối với các đơn vị, cán bộ, viên chức sử dụng máy vi tính tại Trung tâm Y tế huyện Hòa Vang

3. Những hành vi bị nghiêm cấm

- Thu thập, cung cấp, làm lộ, làm mất, chiếm đoạt, mua bán tiêu hủy trái phép tài liệu, thiết bị lưu trữ tin học mang bí mật nhà nước trong Trung tâm.

- Trao đổi, cung cấp tin, tài liệu, thiết bị lưu trữ tài liệu mật cho cơ quan, đơn vị, cá nhân khi chưa được Giám đốc trung tâm phê duyệt.

- Sử dụng máy tính có kết nối mạng Internet để soạn thảo, đánh máy, lưu giữ tài liệu mật; cấm thiết bị lưu giữ bí mật nhà nước vào máy tính có kết nối mạng Internet.

- Sử dụng Micro vô tuyến, điện thoại di động, thiết bị có tính năng ghi âm, thu phát tín hiệu trong cuộc họp có nội dung bí mật nhà nước dưới mọi hình thức, trừ trường hợp được cấp có thẩm quyền cho phép.

- Trao đổi thông tin có nội dung bí mật nhà nước qua mạng xã hội, máy bộ đàm, điện thoại di động, điện thoại kéo dài, máy fax, Internet dưới bất kỳ loại hình dịch vụ nào khi chưa được cấp có thẩm quyền cho phép.

- Cung cấp tin, tài liệu và đưa thông tin thuộc danh mục bí mật nhà nước trên báo chí, ấn phẩm xuất bản công khai, trên cổng thông tin điện tử, trang mạng xã hội, diễn đàn và các hình thức tương tự.

4. Giải thích từ ngữ

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

1. Thiết bị lưu trữ tin học: Những những thiết bị lưu trữ như Ổ cứng rời, USB, đĩa cứng, đĩa mềm dùng để lưu trữ và sao chép, dùng để copy dữ liệu từ máy tính này sang máy tính khác và để lưu giữ dữ liệu.

II./ QUY ĐỊNH CỤ THỂ

1. Soạn thảo, in, sao, chụp tài liệu, thiết bị lưu trữ tài liệu có nội dung mang bí mật nhà nước

Khi soạn thảo, in, sao, chụp tài liệu, vật mang bí mật nhà nước trong ngành Y tế phải thực hiện những quy định sau:

- Tổ chức thực hiện việc soạn thảo, in, sao, chụp tài liệu, vật mang bí mật nhà nước phải tiến hành trong cơ quan, đơn vị, tại nơi an toàn do thủ trưởng cơ quan, đơn vị trực tiếp quản lý tài liệu mật quy định, không mang ra ngoài cơ quan, đơn vị. Khi có yêu cầu, phải soạn thảo trên hệ thống thiết bị đã qua kiểm tra và đủ điều kiện về an toàn, bảo mật. Các đơn vị trong ngành Y tế phải cử cán bộ làm công tác bảo vệ bí mật nhằm theo dõi, quản lý các tin tức, tài liệu mật do cơ quan, đơn vị quản lý;

- Khi soạn thảo văn bản có nội dung bí mật nhà nước, căn cứ nội dung văn bản cá nhân soạn thảo phải đề xuất với thủ trưởng trực tiếp về mức độ mật theo đúng danh mục bí mật nhà nước trong ngành Y tế;

- Với tài liệu mật sao, chụp ở dạng băng, đĩa, phim hoặc bản ghi phải niêm phong và đóng dấu độ mật. Tuyệt đối không đánh máy hoặc in quá số lượng quy định. Sau khi sao, chụp xong phải kiểm tra và hủy bản thảo nếu có. Đối với vật mang bí mật nhà nước phải được niêm phong, có văn bản ghi rõ tên của vật lưu kèm theo và đóng dấu mức độ mật vào văn bản này;

- Khi tổ chức lấy ý kiến tham gia xây dựng dự thảo văn bản, cơ quan chủ trì soạn thảo phải xác định cụ thể phạm vi, đối tượng các cơ quan, tổ chức, cá nhân có liên quan, cần xin ý kiến hoặc tham khảo ý kiến, phải đóng dấu xác định mức độ “mật” cần thiết vào dự thảo trước khi gửi xin ý kiến. Cơ quan, đơn vị, cá nhân nhận được dự thảo phải thực hiện việc quản lý, sử dụng theo đúng độ mật đã ghi trên dự thảo.

2. Gửi tệp tài liệu, thiết bị lưu trữ tin học mang bí mật nhà nước

- Vào sổ: tệp tài liệu, thiết bị lưu trữ tài liệu mật mật trước khi gửi đi phải vào sổ "Tài liệu mật đi". Phải ghi đầy đủ các thông tin sau đây: Số thứ tự, ngày, tháng, năm, nơi nhận, trích yếu nội dung, độ mật, độ khẩn, người nhận (ký tên, ghi rõ họ tên).

- Lập phiếu gửi: tệp tài liệu, thiết bị lưu trữ tài liệu mật mật trong thiết bị lưu trữ tin học gửi đi phải kèm theo phiếu gửi và phải bỏ chung vào bì cùng với thiết bị lưu trữ tài liệu. Phiếu gửi phải ghi rõ nơi gửi, số phiếu, nơi nhận, số ký hiệu từng loại tệp tài liệu, thiết bị lưu trữ tài liệu mật gửi đi, đóng dấu độ mật, khẩn của tệp tài liệu, thiết bị lưu trữ tài liệu mật vào góc phải phía trên của tờ phiếu. Người mở phong bì và người nhận tệp tài liệu, thiết bị lưu trữ tài liệu mật phải ký vào phiếu chuyển để người gửi kiểm tra việc chuyển giao và truy xét kịp thời tệp tài liệu, thiết bị lưu trữ tài liệu mật bị thất lạc.

- Làm bì: tệp tài liệu, thiết bị lưu trữ tài liệu mật mật trong thiết bị lưu trữ tin học gửi đi không được gửi chung trong một phong bì với tệp tài liệu, thiết bị lưu trữ tài liệu mật thường. Giấy làm bì phải là loại giấy dai, khó bóc, khó thấm nước, không nhìn thấu qua được. Gấp bì theo mỗi chéo, hồ dán phải dính, khó bóc.

- Dấu ký hiệu chỉ mức độ tệp tài liệu, thiết bị lưu trữ tài liệu mật mật, tối mật, tuyệt mật đóng ngoài bì.

Không được viết chữ hoặc đóng dấu Mật, Tối mật, Tuyệt mật ở ngoài bì.

+ Tệp tài liệu, thiết bị lưu trữ tài liệu mật có độ “Mật” đóng dấu chữ "C" (con dấu chữ C in hoa nét đậm, nằm trong đường viền tròn, đường kính 1,5 cm).

+ Tệp tài liệu, thiết bị lưu trữ tài liệu mật có độ "Tối mật" đóng dấu chữ "B" (con dấu chữ B in hoa, nét đậm, nằm trong đường viền tròn, đường kính 1,5 cm).

+ Tệp tài liệu, thiết bị lưu trữ tài liệu mật có độ “Tuyệt mật” gửi bằng 02 phong bì:

Bì trong: Do đơn vị soạn thảo văn bản làm, dán kín và ghi rõ số, ký hiệu của tệp tài liệu, thiết bị lưu trữ tài liệu mật, tên người nhận, đóng dấu "Tuyệt mật"; nếu là tệp tài liệu, thiết bị lưu trữ tài liệu mật, vật gửi đích danh người có trách nhiệm giải quyết thì đóng dấu "Chỉ người có tên mới được bóc bì";

Bì ngoài: Do bộ phận văn thư, lưu trữ của cơ quan ghi như tệp tài liệu, thiết bị lưu trữ tài liệu mật thường và đóng dấu ký hiệu chữ “A”(con dấu chữ A in hoa, nét đậm, nằm trong đường viền tròn, đường kính 1,5 cm).

3. Nhận thiết bị lưu trữ tin học có bí mật nhà nước đến

- Khi nhận tệp tài liệu, thiết bị lưu trữ tài liệu mật mật, thiết bị lưu trữ tin học có lưu bí mật nhà nước đến văn thư phải vào sổ "Tệp tài liệu, thiết bị lưu trữ tài liệu mật mật đến" để theo dõi và chuyển đến người có trách nhiệm giải quyết.

- Nếu tệp tài liệu, thiết bị lưu trữ tài liệu mật mật đến mà bì trong có dấu "Chỉ người có tên mới được bóc bì", văn thư vào sổ theo số ký hiệu ghi ngoài bì và chuyển ngay đến người có tên trên bì. Nếu người có tên ghi trên bì đi vắng thì chuyển đến người có trách nhiệm giải quyết, văn thư không được bóc bì.

- Trường hợp tệp tài liệu, thiết bị lưu trữ tài liệu mật mật được gửi đến mà không thực hiện đúng thủ tục bảo mật thì chuyển đến người có trách nhiệm giải quyết, đồng thời báo lại nơi gửi để rút kinh nghiệm. Nếu phát hiện tệp tài liệu, thiết bị lưu trữ tài liệu mật mật gửi đến có dấu hiệu bị bóc, mở bì hoặc tệp tài liệu, thiết bị lưu trữ tài liệu mật bị tráo đổi, mất, hư hỏng, thì người nhận phải báo ngay với thủ trưởng cơ quan, đơn vị để có biện pháp xử lý kịp thời.

- Khi nhận tệp tài liệu, thiết bị lưu trữ tài liệu mật mật, nơi nhận phải hoàn ngay phiếu gửi cho nơi đã gửi tài liệu. Nơi gửi và nơi nhận tệp tài liệu, thiết bị lưu trữ tài liệu mật mật phải tổ chức kiểm tra, đối chiếu thường xuyên nhằm phát hiện những sai sót, mất mát để kịp thời xử lý.

4. Thu hồi tệp tài liệu, thiết bị lưu trữ tài liệu mật có nội dung bí mật nhà nước

Văn thư phải theo dõi, thu hồi hoặc trả lại nơi gửi đúng kỳ hạn tài liệu, vật mang bí mật nhà nước có đóng dấu thu hồi, khi nhận cũng như khi trả đều phải kiểm tra, đối chiếu và xóa sổ để bảo đảm tệp tài liệu, thiết bị lưu trữ tài liệu mật không bị thất lạc.

5. Lưu trữ tệp tài liệu, thiết bị lưu trữ tài liệu mật mang bí mật nhà nước

Tệp tài liệu, thiết bị lưu trữ tài liệu mật "Tuyệt mật", "Tối mật", "Mật" phải được bảo quản, lưu trữ nghiêm ngặt, tổ chức lưu trữ riêng tại nơi có đủ điều kiện, phương tiện bảo quản, bảo đảm an toàn. Nơi cất giữ các loại tệp tài liệu, thiết bị lưu trữ tài liệu mật mật do thủ trưởng cơ quan, đơn vị quy định.

6. Bảo vệ bí mật nhà nước trong thông tin liên lạc

- Không được truyền thông tin nội dung tài liệu mật qua máy mạng xã hội, điện thoại, máy phát sóng, điện báo và máy fax, Internet; trong trường hợp cần thiết được trao đổi bằng điện thoại, fax hoặc bằng phương tiện kỹ thuật khác khi đã được áp dụng các biện pháp bảo mật.

- Thông tin bí mật nhà nước chuyển đi bằng phương tiện viễn thông và máy tính thì phải được mã hóa theo quy định của pháp luật về cơ yếu.

- Tổ Công nghệ thông tin là đơn vị đầu mối hướng dẫn các đơn vị trực thuộc bảo đảm bảo vệ bí mật nhà nước qua mạng Internet, máy tính và thiết bị trực tuyến khác.

7. Chế độ báo cáo, thống kê về công tác bảo mật

Các đơn vị trực thuộc phải thực hiện chế độ báo cáo thống kê về công tác bảo mật như sau:

- Báo cáo đột xuất: Thủ trưởng đơn vị phải báo cáo kịp thời về Ban giám đốc về những vụ việc đột xuất xảy ra. Trong báo cáo cần nêu rõ lý do, nguyên nhân, biện pháp đã tiến hành xử lý, kết quả và ý kiến đề xuất;

- Báo cáo định kỳ công tác hằng năm: Là báo cáo toàn diện về công tác bảo vệ bí mật hằng năm của cơ quan, đơn vị; báo cáo cần ngắn gọn, chính xác, phản ánh đầy đủ tình hình công tác bảo vệ bí mật trong năm;

8. Sử dụng, bảo quản thiết bị lưu trữ tài liệu mật, vật mang bí mật nhà nước

- Các đơn vị trực thuộc có trách nhiệm lập hồ sơ về tài liệu loại "Tuyệt mật", "Tối mật", "Mật" gửi về bộ phận lưu trữ theo quy định của pháp luật.

- Tài liệu mật chỉ được phổ biến trong phạm vi những người có trách nhiệm được biết. Tuyệt đối không được cho người không có trách nhiệm biết khi chưa được thủ trưởng đơn vị cho phép.

- Việc trao đổi tệp tài liệu, thiết bị lưu trữ tài liệu mật hoặc cung cấp số liệu, tin tức mật trên phương tiện thông tin đại chúng phải được Ban giám đốc xét duyệt và chịu trách nhiệm.

- Không được mang thiết bị lưu trữ tài liệu mật ra khỏi nơi lưu giữ; trường hợp đặc biệt nếu được sự đồng ý của người có thẩm quyền có thể mượn và chịu trách nhiệm bảo quản thiết bị lưu trữ tài liệu mật đã mượn và ký nhận vào sổ khai thác tài liệu mật.

- Trường hợp cán bộ phải mang thiết bị có tài liệu mật đi công tác trong nước, công tác nước ngoài, đi họp hay về nhà riêng phải được sự đồng ý của lãnh đạo khoa phòng và phải bảo đảm tuyệt đối an toàn trên đường đi, nơi ở; phải bảo đảm cất giữ thiết bị an toàn, không được làm hư hỏng hoặc mất mát tài liệu. Sau khi hoàn thành nhiệm vụ phải bàn giao tài liệu mật cho bộ phận quản lý.

- Đơn vị được giao nhiệm vụ lưu trữ thiết bị chứa tài liệu mật có trách nhiệm quản lý, sử dụng, bảo quản và cung cấp thông tin một cách kịp thời, trung thực và đúng quy định.

9. Phổ biến, nghiên cứu, sử dụng tài liệu, vật mang bí mật nhà nước

- Phổ biến, nghiên cứu, sử dụng tài liệu, vật mang bí mật nhà nước phải thực hiện theo nguyên tắc sau đây:

+ Độ “Tuyệt mật” chỉ có cá nhân người có thẩm quyền hoặc người được giao nhiệm vụ giải quyết biết;

+ Độ “Tối mật” chỉ phổ biến đến những người, những đơn vị có trách nhiệm giải quyết;

+ Độ “Mật” được phổ biến đến những người, những đơn vị có liên quan đến việc giải quyết, thi hành văn bản;

+ Việc phổ biến, nghiên cứu, sử dụng tài liệu, vật mang bí mật nhà nước phải được thực hiện ở nơi bảo đảm bí mật, an toàn.

+ Đối với các cuộc họp, hội nghị của Trung tâm có nội dung bí mật, chỉ được ghi chép, ghi âm, ghi hình khi được phép của Giám đốc hoặc người có thẩm quyền, Chủ tịch Hội nghị. Các băng ghi âm, ghi hình phải quản lý, bảo vệ như tài liệu gốc.

10. Giải mật tài liệu mật

- Giải mật tài liệu mật là xóa bỏ độ mật đã được xác định của tài liệu mật. Việc giải mật chỉ được xem xét khi nội dung của tài liệu nếu bị tiết lộ không còn gây nguy hại cho Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

- Nguyên tắc, thẩm quyền, trình tự thủ tục giải mật tài liệu mật thực hiện theo quy định của Chính phủ và Bộ Công an.

- Đối với tài liệu lưu trữ lịch sử có nội dung bí mật nhà nước được giải mật theo quy định của Luật lưu trữ và văn bản hướng dẫn thi hành.

11. Tiêu hủy tài liệu mật

- Việc tiêu hủy tài liệu mật sau khi giải mật được thực hiện theo quy định của Luật lưu trữ và các văn bản hướng dẫn thi hành.

- Trong trường hợp đặc biệt không có điều kiện tổ chức tiêu hủy tài liệu mật theo quy định pháp luật hiện hành, nếu tài liệu mật không được tiêu hủy ngay sẽ gây hậu quả nghiêm trọng cho an ninh, quốc phòng hoặc các lợi ích khác của Nhà nước thì người đang quản lý tài liệu mật đó được quyền tự tiêu hủy nhưng ngay sau đó phải báo cáo bằng văn bản cho cấp có thẩm quyền (người đứng đầu cơ quan quản lý tài liệu mật, cơ quan công an cùng cấp). Nếu việc tự tiêu hủy tài liệu mật không có lý do chính đáng thì người tự tiêu hủy phải chịu trách nhiệm trước pháp luật.

III. Trách nhiệm thực hiện

- Việc thực hiện công tác bảo vệ bí mật nhà nước là trách nhiệm của các đơn vị và cá nhân trong toàn trung tâm. Trong phạm vi chức năng, nhiệm vụ, quyền hạn được giao, lãnh đạo các đơn vị trực thuộc, Giám đốc trung tâm tổ chức thực hiện quy định này.

- Tổ công nghệ thông tin tế có trách nhiệm theo dõi, hướng dẫn, kiểm tra, tổng hợp tình hình thực hiện công tác bảo vệ bí mật nhà nước trong toàn trung tâm, báo cáo Ban giám đốc theo quy định.

- Trong quá trình tổ chức thực hiện khi có vướng mắc, đề nghị đơn vị và cá nhân phản ánh bằng văn bản lên Ban giám đốc để xem xét, giải quyết./.

Nơi nhận:

- BGĐ;
- Các đơn vị trực thuộc;
- Lưu: VT, KHTH.

GIÁM ĐỐC

(đã ký)

Nguyễn Đại Vĩnh