BỘ Y TẾ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 7672/QĐ-BYT	*Hà Nội, ngày 26 tháng 12 năm 2018*

QUYẾT ĐỊNH

Cập nhật Kiến trúc Chính phủ điện tử Bộ Y tế phiên bản 1.0

BỘ TRƯỞNG BỘ Y TẾ

Căn cứ Nghị định số 75/2017/NĐ-CP ngày 20/6/2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Y tế;

Căn cứ Quyết định số 5641/QĐ-BYT ngày 31/12/2015 của Bộ trưởng Bộ Y tế về việc ban hành Kiến trúc Chính phủ điện tử Bộ Y tế phiên bản 1.0;

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

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Tài liệu cập nhật Kiến trúc chính phủ điện tử Bộ Y tế phiên bản 1.0". Các nội dung trong tài liệu này là một thành phần của Kiến trúc chính phủ điện tử Bộ Y tế phiên bản 1.0 đã được ban hành kèm theo Quyết định số 5641/QĐ-BYT ngày 31/12/2015 của Bộ trưởng Bộ Y tế.

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

Điều 3. Các Ông, Bà: Cục trưởng Cục Công nghệ thông tin; Chánh văn phòng Bộ; Chánh Thanh tra Bộ; Tổng Cục trưởng; Vụ trưởng; Cục trưởng các Tổng Cục, Vụ, Cục thuộc Bộ Y tế và các tổ chức, cá nhân 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) ;
- Cổng thông tin điện tử Bộ Y tế;
- Lưu: VT, CNTT (02).

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Trường Sơn

BỘ Y TẾ

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

CẬP NHẬT KIẾN TRÚC CHÍNH PHỦ ĐIỆN TỬ BỘ Y TẾ PHIÊN BẢN 1.0

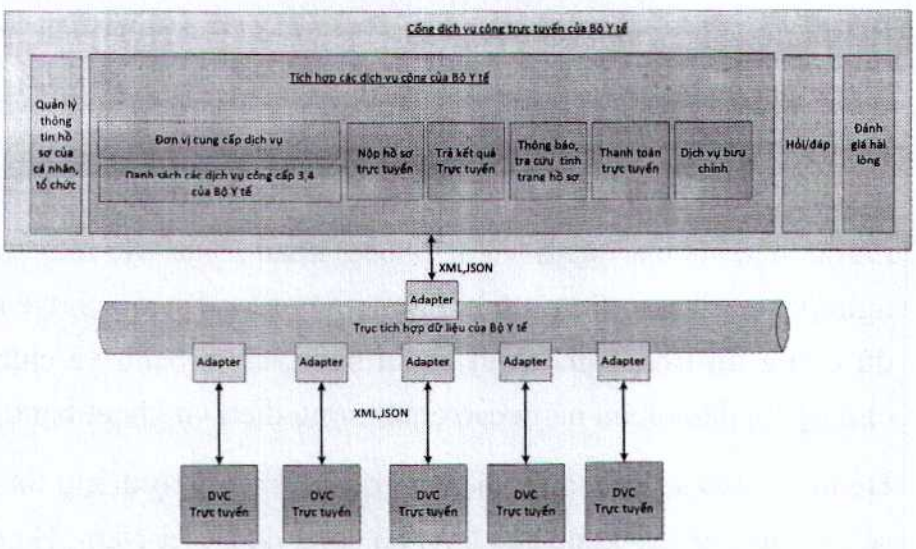
(Ban hành kèm theo Quyết định số 7672/QĐ-BYT ngày 26 tháng 12 năm 2018 của Bộ trưởng Bộ Y tế)

I. Khung kiến trúc tham chiếu cổng dịch vụ công trực tuyến của Bộ Y tế

1. Nguyên tắc

- Cổng dịch vụ công trực tuyến của Bộ Y tế đóng vai trò là cổng duy nhất giao tiếp với người dân, tổ chức, cá nhân bên ngoài cung cấp dịch vụ công trực tuyến của Bộ Y tế.
- Các dịch vụ công trực tuyến của các đơn vị thuộc Bộ Y tế sẽ kết nối với Cổng dịch vụ công trực tuyến của Bộ Y tế để cung cấp thông tin dịch vụ công của đơn vị ra ngoài

2. Các thành phần trong cổng dịch vụ công của Bộ Y tế



3. Mô tả các thành phần

- Quản lý thông tin, hồ sơ của cá nhân và tổ chức: Người giao dịch với Bộ Y tế chỉ thực hiện số hóa và đính kèm thông tin hồ sơ cá nhân một lần (CMND, Giấy chứng nhận đăng ký kinh doanh,…) trên Cổng dịch vụ công; khi thực

hiện nộp hồ sơ lần sau, hồ sơ cá nhân sẽ đính kèm tự động mà không cần thực hiện lại;

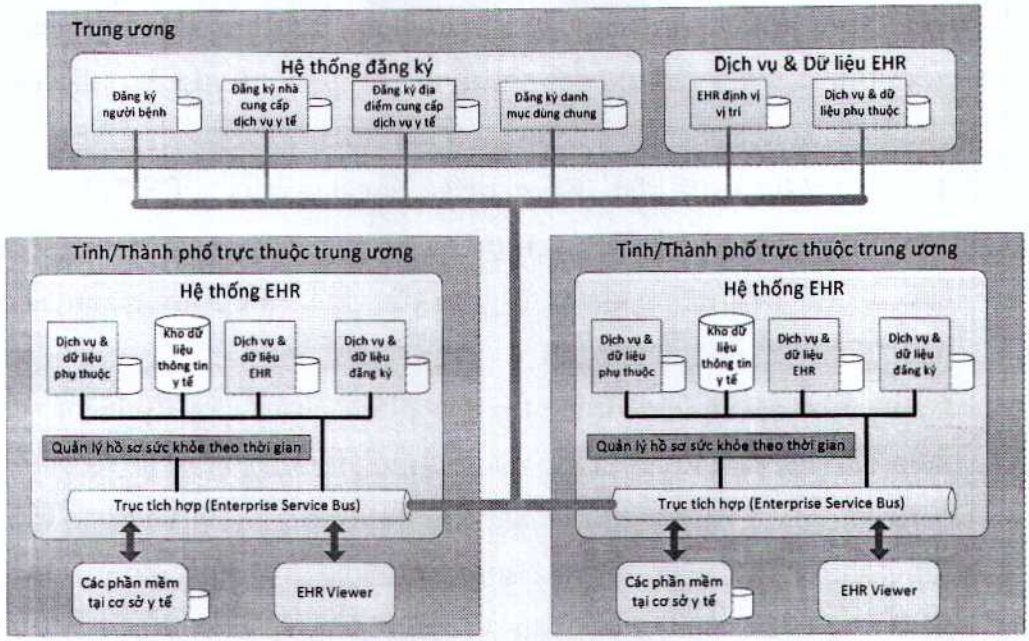
- Tích hợp thông tin, CSDL dịch vụ công trực tuyến của Bộ Y tế và cung cấp cho người dân, doanh nghiệp bao gồm:
    - Thông tin về đơn vị cung cấp dịch vụ, bộ phận Một cửa;
    - Thông tin chi tiết hướng dẫn truy cập và thực hiện các dịch vụ công trực tuyến;
    - Nộp hồ sơ, trả kết quả trực tuyến.
    - Thông báo tình trạng xử lý hồ sơ; công khai, minh bạch tình trạng đúng hạn, trễ hạn các hồ sơ giao dịch trên cổng thông tin;
    - Thực hiện thanh toán lệ phí, thuế;
    - Thực hiện đăng ký dịch vụ bưu chính để nhận hoặc trả hồ sơ tại nhà;
- Hỏi, đáp, hướng dẫn trực tuyến;
- Tiếp nhận, tổng hợp ý kiến đánh giá hài lòng của người dân sử dụng dịch vụ.

II. Khung kiến trúc tham chiếu hệ thống hồ sơ sức khỏe điện tử (EHR)

1. Nguyên tắc

- Hệ thống Hồ sơ sức khỏe điện tử (EHR) là hệ thống quản lý hồ sơ ghi chép tình trạng chăm sóc và lịch sử sức khỏe của một người từ lúc sinh ra cho đến lúc mất đi (đảm bảo tính an toàn và riêng tư của hồ sơ). Hồ sơ sức khỏe này được tạo thành từ nhiều nguồn thông tin/dữ liệu khác nhau bao gồm thông tin/dữ liệu từ các bệnh viện, phòng khám, bác sỹ, nhà thuốc, phòng xét nghiệm, … Thông tin rất quan trọng này sẽ giúp các chuyên gia y tế có đầy đủ thông tin trong quá trình khám bệnh, chữa bệnh và chăm sóc sức khỏe cho người dân nhằm nâng cao chất lượng dịch vụ khám bệnh, chữa bệnh
- Hệ thống Hồ sơ sức khỏe điện tử quản lý toàn bộ thông tin tình trạng chăm sóc và lịch sử sức khỏe của toàn bộ công dân Việt Nam. Hệ thống Hồ sơ sức khỏe điện tử do Bộ Y tế quản lý và được quản lý, vận hành tập trung tại trung tâm dữ liệu của Bộ Y tế

2. Các thành phần của hệ thống hồ sơ sức khỏe điện tử



Các chức năng cơ bản của hệ thống hồ sơ sức khỏe điện tử

- **Các hệ thống đăng ký**: Cung cấp dịch vụ đăng ký cho các cá nhân và các thực thể kết nối, giao tiếp với hệ thống hồ sơ sức khỏe cá nhân bao gồm người bệnh, nhà cung cấp dịch vụ y tế, địa điểm cung cấp dịch vụ y tế, danh mục dùng chung.
- **Dịch vụ Quản lý hồ sơ sức khỏe theo thời gian**: Dịch vụ này cho phép điều phối và thực hiện bất kỳ giao dịch nào để cung cấp tất cả thông tin/dữ liệu dữ liệu lâm sàng của người bệnh theo chiều thời gian:
    - Quản lý và lưu trữ dữ liệu người bệnh trong kho lưu trữ EHR
    - Kiểm tra, xác nhận dữ liệu và định dạng thông tin phản hồi
    - Chuẩn hóa nội dung dữ liệu
    - Quản lý tiến trình tương tác của EHR
    - Duy trì thông tin tóm tắt về nội dung sự kiện và vị trí của người bệnh
- **Kho lưu trữ Bản ghi Y tế có thể được chia sẻ**: duy trì dữ liệu lịch sử về các lần khám bệnh, chữa bệnh cùng với các dữ liệu lâm sàng. Ví dụ về các lớp dữ liệu có thể bao gồm lần khám bệnh, chữa bệnh hoặc truy cập các tài liệu tóm tắt, yêu cầu chuyển viện và ghi chú, dữ liệu chẩn đoán, quan sát, các phác đồ điều trị, kế hoạch điều trị;

- **Các kho lưu trữ theo lĩnh vực**: lưu trữ, duy trì và cung cấp tập hợp các thông tin/dữ liệu lâm sàng liên quan đến bức tranh lâm sàng của người bệnh gồm thuốc hoặc đơn thuốc, chỉ định xét nghiệm và kết quả xét nghiệm, các chỉ định và kết quả chẩn đoán hình ảnh, …
- **Trục tích hợp dữ liệu (Enterprise Service Bus – ESB)** bao gồm các dịch vụ thông dụng và kênh truyền thông nhằm tạo môi trường kết nối liên thông, chia sẻ dữ liệu/thông tin y tế giữa các phần mềm ứng dụng PoS với EHR hoặc giữa các hệ thống EHR.
- **Các phần mềm ứng dụng tại địa điểm cung cấp dịch vụ y tế** (PoS) đại diện cho tất cả các hệ thống đang được sử dụng bởi các tổ chức hoặc người cung cấp dịch vụ y tế thực hiện việc lưu trữ, quản lý và cung cấp dữ liệu lâm sàng cho người bệnh nhân. Các phần mềm ứng dụng PoS tương tác với một hệ thống EHR trong một phạm vi nhất định. Sự tương tác này được thực hiện thông qua việc trao đổi các bản tin giữa các ứng dụng thông qua Trục tích hợp dữ liệu.

- **Dịch vụ & dữ liệu phụ thuộc**: Các dịch vụ nhóm này thường đòi hỏi phải có sự hiện diện của dữ liệu cốt lõi trong hệ thống EHR và có thể mang lại giá trị gia tăng cho các dữ liệu đó để hỗ trợ các chức năng đặc biệt của hệ thống y tế. Các ví dụ hiện tại bao gồm các dịch vụ liên quan đến Giám sát Y tế Công cộng chẳng hạn như Quản lý Bùng phát và Báo cáo Bệnh truyền nhiễm. Trong tương lai, nhóm dịch vụ này có thể kết hợp các khả năng như các dịch vụ quản lý thời gian chờ hoặc các dịch vụ lập kế hoạch tổng thể.

III. Khung kiến trúc tham chiếu hệ thống thông tin quản lý trạm y tế xã, phường, thị trấn

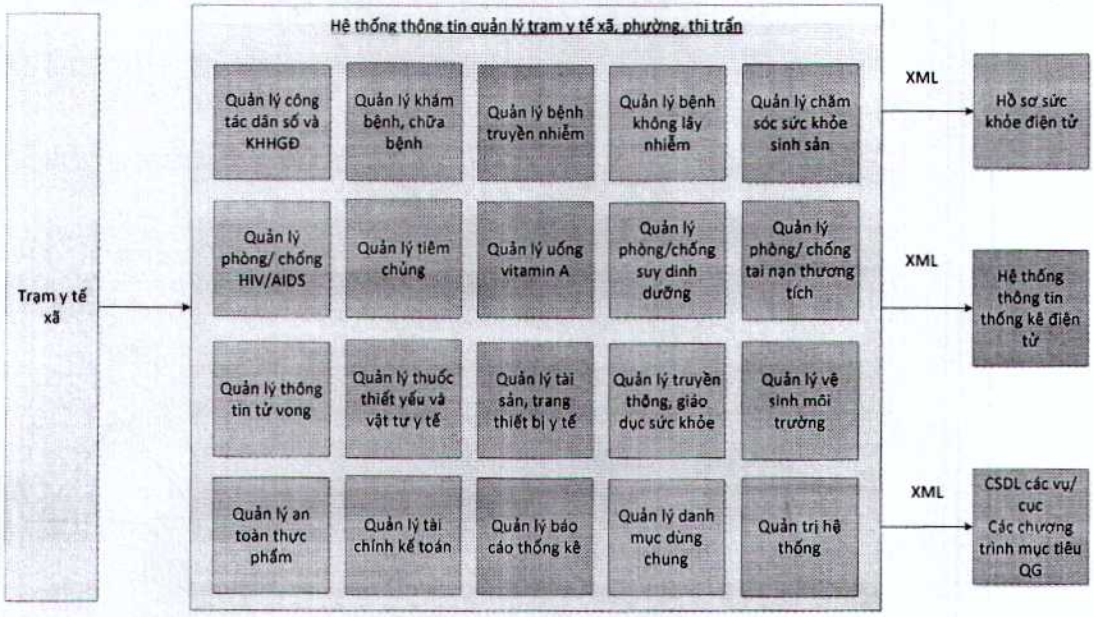
1. Nguyên tắc

- hệ thống thông tin quản lý trạm y tế xã, phường, thị trấn quản lý toàn bộ hoạt động của trạm y tế xã. Các cán bộ tại trạm y tế xã chỉ sử dụng duy nhất hệ thống thông tin quản lý trạm y tế xã, phường, thị trấn trong các hoạt động nghiệp vụ của mình.

- hệ thống thông tin quản lý trạm y tế xã, phường, thị trấn sẽ chuyển các thông tin liên quan đến người bệnh tại trạm y tế xã cho phần mềm hồ sơ sức khỏe điện tử.
- hệ thống thông tin quản lý trạm y tế xã, phường, thị trấn sẽ chuyển các thông tin thống kê liên quan đến hệ thống thống kê y tế điện tử

2. Các thành phần của phần mềm quản lý trạm y tế xã

- Các thành phần của phần mềm quản lý trạm y tế xã tuân thủ theo quy định tại quyết định số 6110/QĐ-BYT ngày 19/12/2017 của Bộ trưởng Bộ Y tế ban hành hướng dẫn xây dựng và triển khai hệ thống thông tin quản lý trạm y tế xã, phường, thị trấn



IV. Khung kiến trúc tham chiếu hệ thống thông tin thống kê điện tử

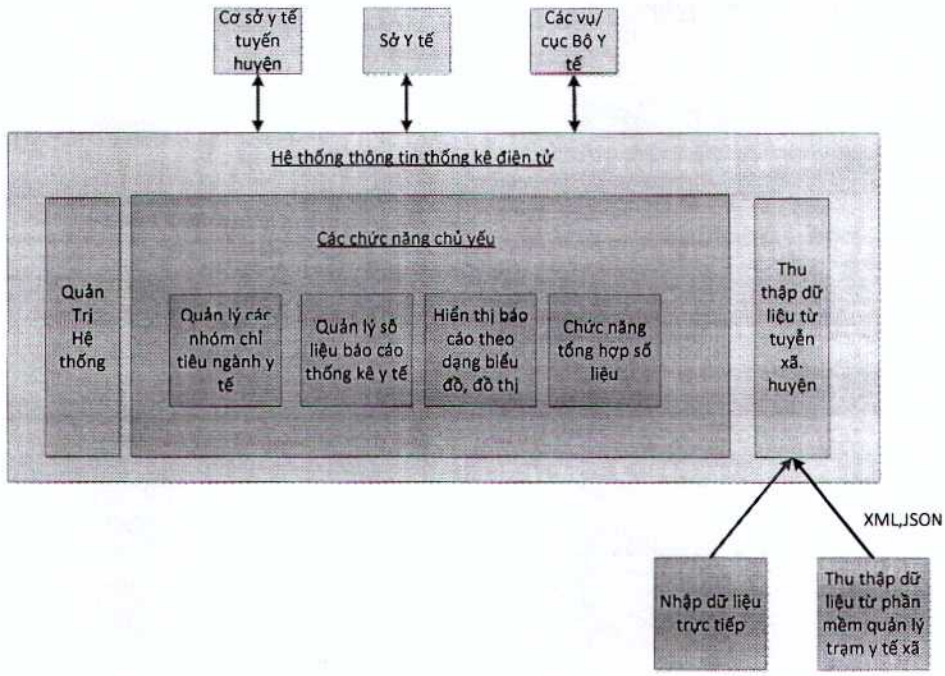
1. Nguyên tắc

- Hệ thống thống kê điện tử tin học hóa các quy trình nghiệp vụ của công tác thống kê y tế theo theo các quy định sau:
  - Thông tư 27/2014/TT-BYT Quy định hệ thống biểu mẫu thống kê y tế cơ sở y tế tuyến tỉnh huyện xã
  - Thông tư 28/2014/TT-BYT Quy định nội dung hệ thống chỉ tiêu thống kê ngành Y tế

- Thông tư 32/2014/TT-BYT Ban hành danh mục chỉ tiêu thống kê y tế cơ bản áp dụng cho tuyến tỉnh huyện xã

- Hệ thống thông tin thống kê điện tử thu thập các thông tin từ tuyến xã, huyện tổng hợp lên kho dữ liệu đặt tại trung tâm dữ liệu của Bộ Y tế
- Số liệu thu thập và phân tích được quản lý trong hệ thống thông tin thống kê y tế điện tử là cơ sở cho việc khai thác, tra cứu, lập báo cáo của tuyến huyện, tuyến tỉnh của các tỉnh, thành phố trực thuộc trung ương ; các vụ, cục chuyên ngành của Bộ Y tế.

2. Các thành phần của hệ thống thông tin thống kê y tế



3. Các thành phần của hệ thống thông tin thống kê y tế điện tử

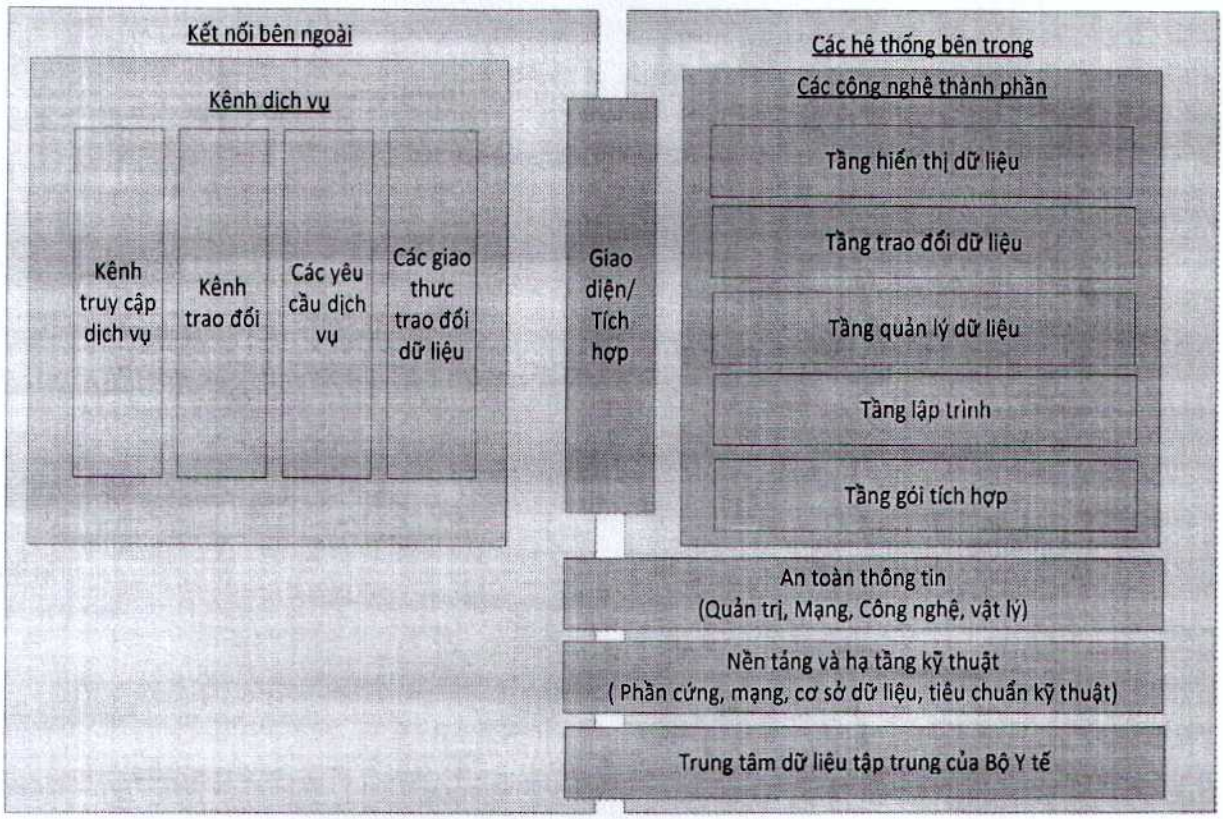
- Thành phần quản trị hệ thống : Quản trị người sử dụng, quản trị truy cập hệ thống
- Thành phần quản lý các nhóm chỉ tiêu ngành y tế quản lý các nhóm chỉ tiêu sau :
    - Thông tư 28/2014/TT-BYT Quy định nội dung hệ thống chỉ tiêu thống kê ngành Y tế
    - Thông tư 32/2014/TT-BYT Ban hành danh mục chỉ tiêu thống kê y tế cơ bản áp dụng cho tuyến tỉnh huyện xã

- Thành phần quản lý các biểu mẫu báo cáo theo các mẫu báo cáo tại thông tư
    - Thông tư 27/2014/TT-BYT Quy định hệ thống biểu mẫu thống kê y tế cơ sở y tế tuyến tỉnh huyện xã
    - Các mẫu báo cáo đặc thù khác
- Thành phần hiển thị báo cáo theo dạng đồ thị, biểu đồ
- Thành phần thu thập dữ liệu bao gồm
    - Thành phần làm sạch dữ liệu
    - Chức năng nhập dữ liệu theo mẫu
    - Chức năng tích hợp lấy dữ liệu từ phần mềm trạm y tế xã
- Chức năng tổng hợp dữ liệu để lập báo cáo và hiển thị dữ liệu

V. Mô hình tham chiếu công nghệ

1. Các thành phần mô hình tham chiếu công nghệ

Các thành phần của mô hình tham chiếu công nghệ của Bộ Y tế được mô tả ở mô hình sau :



Mô tả các thành phần :

- **Kênh dịch vụ**: Đặc tả nhóm các tiêu chuẩn hỗ trợ truy xuất bên ngoài từ người sử dụng.
- **Công nghệ thành phần**: xác định nền tảng cơ bản và các yếu tố kỹ thuật mà các thành phần dịch vụ được xây dựng, tích hợp và triển khai trên các kiến trúc dựa trên thành phần. Khung thành phần bao gồm việc thiết kế ứng dụng hoặc phần mềm hệ thống kết hợp các giao diện để tương tác với các chương trình khác và tính linh hoạt trong tương lai và khả năng mở rộng
- **Giao diện và tích hợp**: Quy định công nghệ và cách thức giao tiếp giữa đơn vị và hệ thống.
- **An toàn thông tin**: định nghĩa cách thức đảm bảo an toàn thông tin cho toàn bộ hệ thống
- **Nền tảng và hạ tầng**: bao gồm phần cứng, mạng, cơ sở dữ liệu, tiêu chuẩn công nghệ

2. Các yêu cầu đối với các thành phần của mô hình tham chiếu công nghệ

a) Kênh dịch vụ

Nhóm dịch vụ	Yêu cầu
Kênh truy cập dịch vụ	Chạy được trên các trình duyệt web khác nhau bao gồm: Microsoft IE, Mozilla, Google Chrome, Opera
	Truy nhập được từ các kênh di động bao gồm điện thoại di động, máy tính bảng, thiết bị PDA
	Truy cập được tư các kênh truyền thông gồm thư điện tử, Fax, VOIP, Kiosk, Mạng xã hội

Nhóm dịch vụ	Yêu cầu
Kênh trao đổi	Mạng LAN của Bộ Y tế
	Internet
	Mạng số liệu chuyên dùng
Các Yêu cầu dịch vụ	Các hướng dẫn, quy định trong việc truy cập bao gồm chính sách an toàn thông tin, chính sách truy cập trang web, các chính sách truy cập phần mềm ứng dụng. Các chính sách về việc vận hành, khai thác trung tâm dữ liệu ngành Y tế
	Dịch vụ đám mây được triển khai để có thể truy cập trong mạng nội bộ, qua internet, hoặc mạng số liệu chuyên dùng bao gồm SaaS (Software as a Service), PaaS (Platform as a Service) ,IaaS (infrastructure as a Service)
	Các giao thức ứng dụng
Các dịch vụ giao thức kết nối	Hỗ trợ các giao thức kết nối bao gồm : IMAP, POP3, MIME, SMTP, SNMP, LDAP, X.500, BGP, DHCP, DNS, HTTP, WAP, FTP
	Hỗ trợ các giao thức mạng : TCP, IPv4, IPv6, UDP, IPSEC

b) Nền tảng và hạ tầng

Nhóm dịch vụ	Yêu cầu
Mạng	Mạng cục bộ được triển khai đầy đủ tại các đơn vị Tất cả các đơn vị đều được kết nối Internet tốc độ cao Đầy đủ thiết bị mạng phục vụ hoạt động không gián đoạn tại các đơn vị Đảm bảo thiết bị không dây đầy đủ, hiệu quả tại các đơn vị Đảm bảo vận hành, khai thác hệ thống Video conference của Bộ Y tế
Phần cứng	- Máy chủ đủ công suất, hiệu năng, đáp ứng tính sẵn sàng trên 95% cho các ứng dụng dùng chung. Máy chủ chạy cơ chế sẵn sàng cao - Đủ các thiết bị máy tính cá nhân, Đảm bảo đủ máy in, máy scan cho các đơn vị trong ngành kiểm sát. - Đảm bảo thiết bị lưu trữ đầy đủ cho các cơ sở dữ liệu và phần mềm dùng chung tại cơ quan Bộ Y tế.
Cơ sở dữ liệu	- Cơ sở dữ liệu SQL cho việc lữu trữ các dữ liệu có cấu trúc. - Cơ sở dữ liệu NoSQL cho việc lưu trữ các dữ liệu phi cấu trúc.

Nhóm dịch vụ	Yêu cầu
	- Cơ sở dữ liệu lớn - Sử dụng Cơ sở dữ liệu có bản quyền đảm bảo tính đầy đủ chức năng, tính bảo mật, tính hiệu năng của cơ sở dữ liệu
Máy chủ hỗ trợ dịch vụ	- Máy chủ Web - Máy chủ ứng dụng - Máy chủ đa phương tiện - Máy chủ cho cổng thông tin - Máy chủ Cache - Máy chủ Proxy - Máy chủ thư mục - Máy chủ định danh
Các nền tảng hỗ trợ	- Đảm bảo nền tảng phát triển chạy trên mọi môi trường (Web, Mobile)
Ảo hóa	- Sử dụng các công nghệ ảo hóa máy chủ - Sử dụng các công nghệ ảo hóa ứng dụng - Sử dụng các công nghệ ảo hóa sao lưu
Quản lý hệ thống	- Quản lý cấu hình hệ thống - Quản lý thay đổi - Quản lý sự cố - Quản lý tính sẵn sang - Quản lý tính liên tục của dịch vụ - Quản lý trạng thái

Nhóm dịch vụ	Yêu cầu
	- Quản lý hiệu năng - Quản lý năng lực - Quản lý lỗi - Quản lý Backup - Quản lý các mức dịch vụ
Công nghệ phần mềm	- Quản lý chất lượng và cấu hình phần mềm - Quản lý kiểm thử phần mềm - Quản lý thay đổi, nâng cấp phần mềm - Phương pháp luận phát triển phần mềm: Hướng dịch vụ - Sử dụng các nền tảng lập trình web dotnet, Oracle Developer, Java. - Sử dụng các nền tảng lập trình di động Angular JS, Node JS, React Js,..

c) Công nghệ thành phần

Nhóm dịch vụ	Chi tiết công nghệ
Trình bày dữ liệu	- Đơn giản, dễ sử dụng - Có thể lấy dữ liệu tĩnh hoặc động - Có thể trình bày dữ liệu trên nền tảng web và nền tảng di động - Sử dụng font chữ tiếng Việt
Quản lý dữ liệu	- Xây dựng Metadata của dữ liệu cho việc quản lý dữ liệu

Lập trình	- Độc lập công nghệ

d) Giao diện và tích hợp

Nhóm dịch vụ	Chi tiết công nghệ
Kết nối và tích hợp dịch vụ	- Middleware, EAI, Web Services, ESB, API Gateway
Chia sẻ dữ liệu	- Phải quy định và công bố cấu trúc dữ liệu khi chia sẻ dữ liệu cho các đơn vị. - Sử dụng các tiêu chuẩn dữ liệu chuyên ngành y tế tại quyết định số 2035/QĐ-BYT ngày 12/06/2013 của Bộ trưởng Bộ Y tế về việc công bố danh mục kỹ thuật về ứng dụng công nghệ thông tin trong lĩnh vực y tế.
Giao diện dịch vụ	- UDDI - WSDL - API - Web Service

e) An toàn thông tin

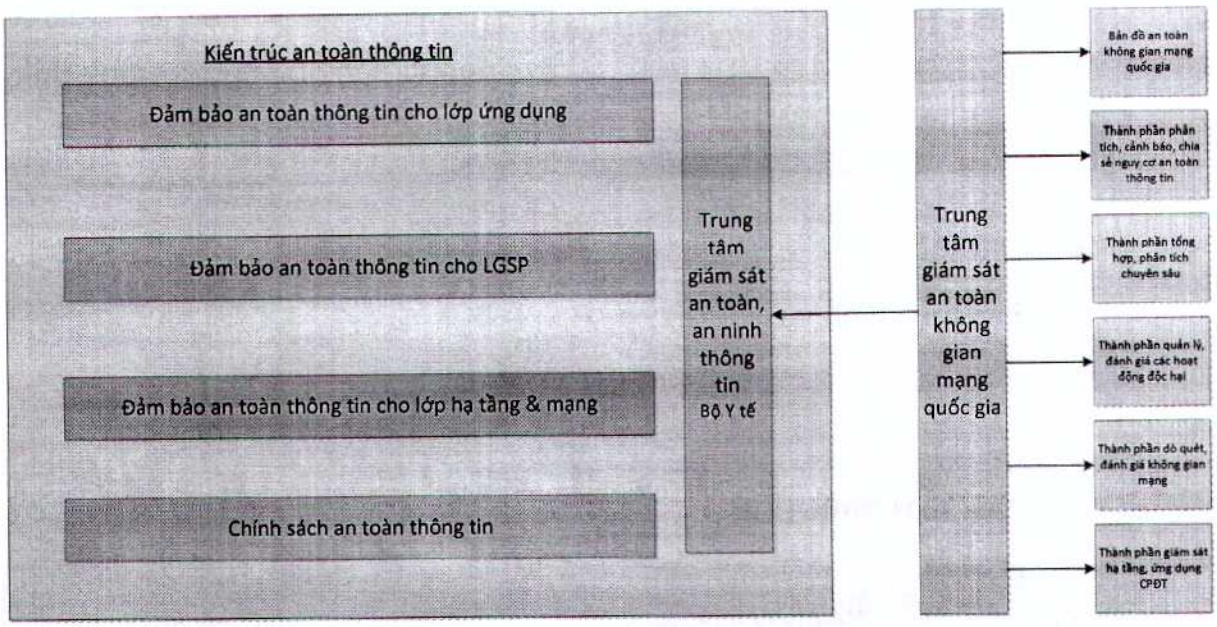
Nhóm dịch vụ	Chi tiết công nghệ
An toàn thông tin mức ứng dụng	- Kiểm tra Code khi lập trình, khi nghiệm thu cài đặt phần mềm - Quản lý truy cập phần mềm theo Role-Based - Khuyến khích hai lớp truy cập đối với dữ

	liệu quan trọng
An toàn thông tin mức hạ tầng	- An toàn thông tin mạng - An toàn thông tin hệ thống - Giám sát an toàn thông tin
An toàn thông tin mức vật lý	- Bảo vệ cửa ra vào nơi đặt máy chủ - Có chế độ lưu trữ, phục hồi tại hai địa điểm.

3. Kiến trúc tham chiếu an toàn thông tin

a) Các thành phần

Kiến trúc tham chiếu an toàn thông tin của Bộ Y tế được thể hiện ở mô hình sau :



Nội dung 1 : Đảm bảo an toàn thông tin cho lớp ứng dụng

- Bảo vệ máy chủ hệ thống
- Bảo vệ ứng dụng web
- Bảo vệ máy chủ cơ sở dữ liệu
- Bảo vệ thư điện tử

- Phòng chống virus và mã độc
- Bảo vệ hệ thống Video conference
- Bảo vệ truy cập Cổng thông tin điện tử
- Triển khai hệ thống chữ ký số xác thực người sử dụng trong các hệ thống văn bản điều hành, thư điện tử, các hệ thống ứng dụng chuyên dùng.

Nội dung 2: Đảm bảo an toàn thông tin cho nền tảng tích hợp dữ liệu LGSP

- Quản lý an toàn định danh
- Quản lý an toàn xác thực
- Quản lý an toàn cấp quyền truy cập
- Quản lý an toàn dịch vụ tích hợp
- Quản lý an toàn trao đổi thông tin, dữ liệu

Nội dung 3: Đảm bảo an toàn hạ tầng kỹ thuật

Bảo vệ vành đai, chống tấn công từ bên ngoài vào

- Chống tấn công từ chối dịch vụ
- Tường lửa, mạng riêng ảo, ngăn chặn xâm nhập, lọc nội dung, ngăn ngừa mã độc hại, kiểm soát ứng dụng, kiểm soát người dùng
- Kiểm soát nội dung và bảo vệ người dùng Internet.

Bảo vệ mạng nội bộ

- Triển khai các giải pháp bảo vệ hệ thống mạng nội bộ

Nội dung 4: Giám sát An toàn thông tin

Xây dựng trung tâm giám sát an toàn thông tin bao gồm các nội dung sau đây:

- Giải pháp giám sát, theo dõi các mạng và HTTT
- Giám sát, theo dõi mã độc và tấn công vào hệ thống mạng.
- Giải pháp quản lý nhật ký và sự kiện an toàn thông tin, nhằm mục đích thu thập nhật ký từ tất cả các hệ thống, cung cấp đa dạng và linh hoạt các

công cụ cho việc tìm kiếm, phân tích, theo dõi các sự kiện an ninh theo thời gian thực

- Kết nối với trung tâm giám sát an toàn không gian mạng Quốc gia

Nội dung 5: Chính sách an toàn thông tin

- **Quy định về kiểm soát truy cập vật lý**: Nhằm ngăn cản những truy cập bất hợp pháp vào máy chủ, máy tính cá nhân, thiết bị phần cứng và giảm thiểu thiệt hại đối với các thông tin quan trọng
- **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.
- **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.
- **Quy định về 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.
- **Quy định về việc quản lý bên thứ 3**: 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
- **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.

b) Công nghệ áp dụng :

1. Vùng ngoại vi
Triển khai các giải pháp bảo mật cho vùng biên (Internet, vùng kết nối

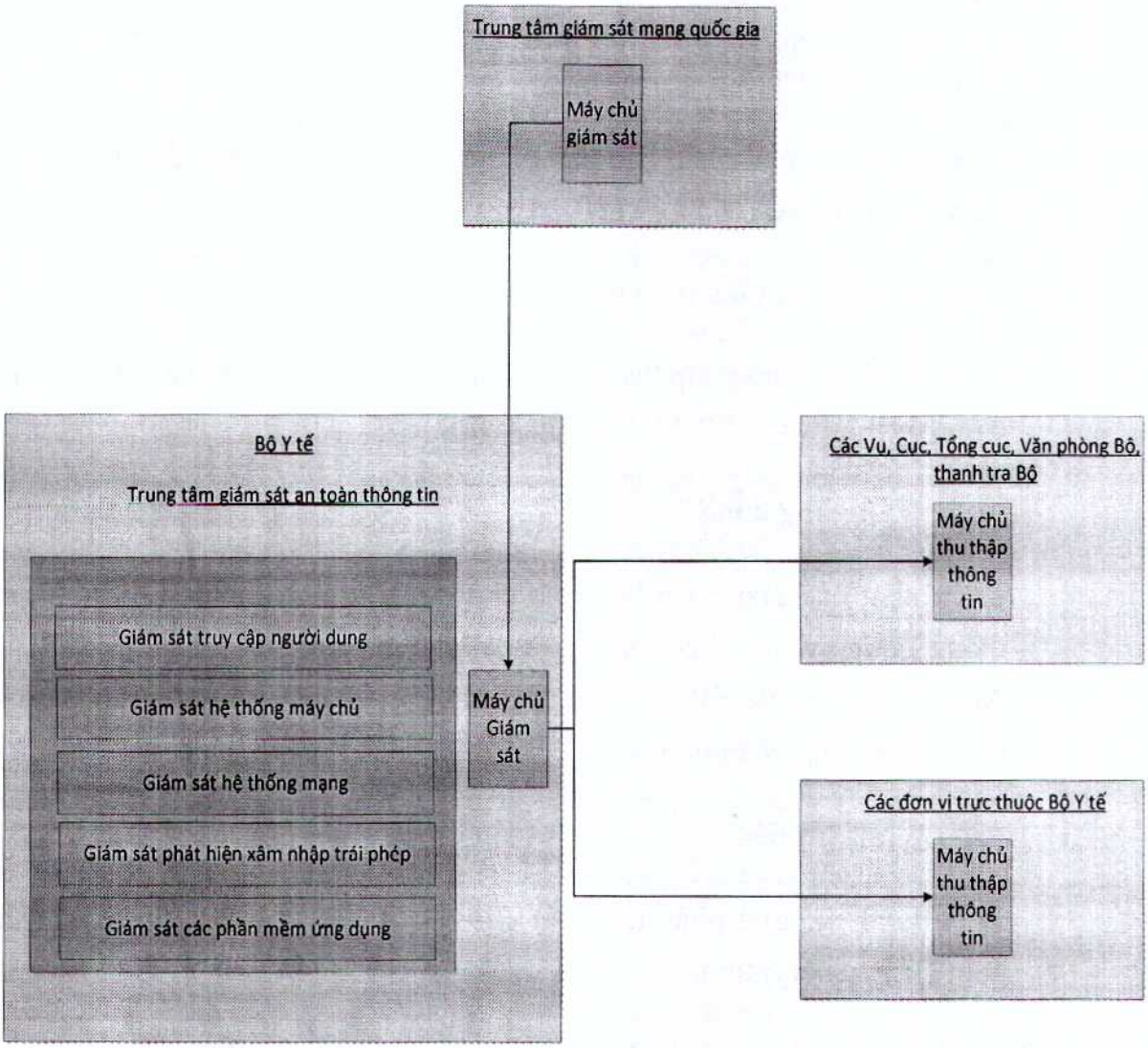
WAN) bao gồm : Firewall, Network IPS, Web filter, hệ thống VPN, Anti DDOS
2. Vùng mạng nội bộ
Triển khai các giải pháp bảo mật cho các vùng mạng nội bộ như User, WIFI, Server , NAC, AAA, Firewall.
3. Vùng máy chủ, thiết bị đầu cuối
Triển khai các giải pháp bảo mật, kiểm soát các tiến trình cho máy trạm, máy chủ AntiMalware, SIEM, PIM, host IPS.
4. Vùng ứng dụng
Triển khai các giải pháp bảo mật cho các ứng dụng như web, mail, các hệ thống ứng dụng bao gồm: WAF, Email Security, Firewall, Open Authentication, hệ thống quản lý và cập nhật bản vá tập trung, hệ thống chống tấn công có chủ đích ATP, hệ thống xác thực đa nhân tố.
5. Vùng dữ liệu
Triển khai các giải pháp bảo mật cho dữ liệu, chống thất thoát dữ liệu bao gồm DLP, Encryption.

c) Kiến trúc tham chiếu hệ thống giám sát an toàn thông tin

Nguyên tắc :

- Hệ thống giúp thu thập và phân tích, giám sát tập trung toàn hệ thống, dựa vào sự tương quan đưa ra các cảnh báo thời gian thực về các mối nguy hại, tấn công vào hệ thống, đưa ra các báo cáo định kỳ, tuân thủ tiêu chuẩn bảo mật quốc tế
- Hệ thống có khả năng thu thập, phân tích, giám sát và gửi cảnh báo về các sự kiện bảo mật của tất cả các đơn vị thuộc, trực thuộc Bộ Y tế.

Kiến trúc của trung tâm giám sát an toàn an ninh



Các nội dung giám sát

- Giám sát liên tục và thống nhất: cung cấp môi trường giám sát đầu cuối thời gian thực, cung cấp khả năng xử lý các vấn đề, giám sát tính sẵn sàng và dung lượng tài nguyên (Event, performance, topology, inventory…), báo cáo thống kê.
- Giám sát các chương trình phần mềm, dịch vụ hoạt động trên hệ thống.
- Giám sát hiệu năng hoạt động của máy chủ cơ sở dữ liệu, máy chủ email.
- Xác định nguồn lưu lượng đi ra/vào hệ thống, thu thập thông tin cụ thể, chính xác.

- Thực hiện quản lý và giám sát các hệ thống máy chủ ảo hoá.
- Liên kết sự kiện và phân tích nguồn gốc lỗi: tự động thu thập các thông tin về sự kiện, phân tích lỗi thông qua các sự kiện và cảnh báo từ các nguồn giám sát.
- Giải pháp tích hợp: các thành phần của giải pháp có khả năng mở rộng và tích hợp với các thành phần khác (reporting, trouble ticket…)

4. Các thành phần nền tảng và hạ tầng kỹ thuật

Với độ phức tạp về yêu cầu đối với hạ tầng CNTT đến từ Kiến trúc ứng dụng, Kiến trúc dữ liệu, khả năng mở rộng, tính sẵn sàng cao, các yêu cầu về quản lý chất lượng dịch vụ, khả năng tuân thủ cũng như việc vận hành hạ tầng công nghệ thông tin cho thấy không có duy nhất một kiến trúc duy nhất nào đáp ứng được.

Chưa kể đến các yêu cầu đến từ việc thu thập hồ sơ vụ án từ các Viện kiểm sát với lượng dữ liệu phát sinh lớn, nhu cầu về kết nối mạng cực lớn.

Vì thế, khi xây dựng hạ tầng kỹ thuật của Bộ Y tế sẽ tiếp cận theo cách xây dựng từng khối hạ tầng và cung cấp dưới dạng dịch vụ, đi kèm với các tiêu chuẩn về kiểm soát, chất lượng dịch vụ, an toàn an ninh thông tin nhằm đảm bảo đáp ứng được việc cung cấp một hạ tầng CNTT phục vụ các nhu cầu của Bộ Y tế từ hiện tại đến tương lai.

Các khối hạ tầng kỹ thuật của Bộ Y tế bao gồm :

a) Hạ tầng tính toán:

- Cung cấp đủ năng lực xử lý, tính toán thông tin, dữ liệu, vận hành ứng dụng
- Với các xu hướng phát triển về nhu tính toán gần đây như trí tuệ nhân tạo, máy học, v.v…, yêu cầu về tải đối với năng lực tính toán tăng càng lúc càng nhanh, gần như tuyến tính và trong một số trường hợp khả năng tính toán về CPU không còn đủ khả năng đáp ứng mà cần phải kết hợp với tính toán bằng chip xử lý đồ họa (GPU).

Điện toán đám mây – Cloud Computing:

- Phục vụ các nhu cầu tính toán thông thường, được cung cấp dưới dạng dịch vụ.
- Việc tích hợp sẵn các phần mềm quản trị, công cụ theo dõi giúp hạ tầng điện toán đám mây có khả năng giúp người dùng cuối tự phục vụ (self-service), giảm bớt các yêu cầu vận hành đơn giản và khả năng mở rộng khi cần gần như không giới hạn.
- Đáp ứng các nhu cầu về các platform thông dụng, các nền tảng xây dựng và vận hành ứng dụng đến từ kiến trúc ứng dụng và kiến trúc dữ liệu thông thường. Hầu hết các ứng dụng và dữ liệu sẽ vận hành trên hạ tầng này. Ví dụ: Web services, Application server, Windows server, Linux server, v.v…

Máy chủ vật lý hội tụ và siêu hội tụ

- Đối với một số trường hợp rất đặc thù như nhu cầu xử lý một khối dữ liệu y tế lớn hoặc các dữ liệu dưới dạng phi cấu trúc, Bộ y tế cần triển khai Các máy chủ hội tụ và siêu năng lực xử lý rất lớn hoặc rất đặc biệt như:

  + GPU base computing;

  + Deep-learning;

  + In-memory computing.

- Các máy chủ hội tụ và siêu hội tụ có khả năng mở rộng, nâng cấp dễ dàng, tối đa hóa năng lực của điện toán đám mây
- Chủ động hợp nhất các lớp phần cứng như máy chủ tính toán (computing), thiết bị chuyển mạch lưu trữ (SAN Switch) và hệ thống lưu trữ (Storage Arrays) vào một thiết bị duy nhất.
- Các máy chủ sẽ được kết nối cài đặt triển khai nền tảng điện toán đám mây riêng để có thể triển khai được các dịch vụ của điện toán đám mây bao gồm :

+ Cung cấp nền tàng phần mềm dưới dạng dịch vụ : SaaS (Software at a Service)

+ Cung cấp nền tảng phát triển dưới dạng dịch vụ : PaaS (Platform as a Service)

+ Cung cấp hạ tầng dưới dạng dịch vụ : IaaS (Infrastructure as a Service)

b) Hạ tầng kết nối mạng

Cung cấp khả năng kết nối các thiết bị, bao gồm cả kết nối giữa hạ tầng tính toán với hạ tầng lưu trữ, hạ tầng tính toán với người dùng

Hạ tầng mạng trung tâm dữ liệu:

- Có tính sẵn sàng cao, độ trễ rất thấp, cung cấp hạ tầng kết nối cho:

+ Hạ tầng tính toán với hạ tầng lưu trữ;

+ Hạ tầng tính toán với người dùng cuối;

+ Hạ tầng tính toán với hạ tầng tính toán biên (edge computing).

+ Hạ tầng điện toán đám mây.

Hạ tầng mạng tại các đơn vị thuộc, trực thuộc Bộ Y tế

- Là mạng nội bộ (LAN), cung cấp kết nối cho người dùng và thiết bị đầu cuối tại các Viện kiểm sát nhân dân. Người dùng có thể truy cập vào mạng nội bộ bằng mạng không dây hoặc mạng có dây.
- Mạng nội bộ của các đơn vị phải có khả năng kết nối đến Trung tâm dữ liệu của Bộ Y tế với tính sẵn sàng cao: kết nối từ internet thông qua kỹ thuật tạo mạng riêng ảo. Thông tin truyền dẫn giữa các đơn vị với TTDL phải được mã hóa.
- Thiết kế mạng nội bộ cần hướng đến khả năng hợp nhất truy cập và quản trị (truy cập và quản trị mạng có dây hay không dây như một hạ tầng thống nhất).

- Thiết kế mạng nội bộ phải đảm bảo hiệu năng phù hợp, có tính sẵn sàng cao, có khả năng chịu lỗi kể cả khi xảy ra các sự cố hỏng hóc về phần cứng.
- Thiết kế mạng nội bộ phải đảm bảo khả năng bảo mật ở nhiều lớp: bảo mật đầu cuối (giải pháp chống thất thoát, tường lửa cá nhân, tính năng phát hiện và chống xâm nhập đầu cuối, phòng chống virus v.v…), phân tách và kiểm soát giữa các lớp mạng nội bộ cũng như bên ngoài mạng (VLAN, tường lửa, proxy …) , khả năng phát hiện chống tấn công và xâm nhập (IPS), khả năng hiện thị, kiểm soát và ghi nhật kí (ví dụ như netflow, syslog, hardware DPI v.v…)
- Mạng nội bộ có khả năng đáp ứng tốt các dịch vụ như hội họp trực tuyến, dịch vụ thoại bằng IP, dịch vụ truyền hình IP hay các ứng dụng truyền thông theo thời gian thực khác.
- Có khả năng ảo hóa mạng chuyển mạch cũng như hỗ trợ tốt cho các nền tảng ảo hóa khác.
- Một số tiêu chuẩn quốc tế /gia thức tối thiểu mà mạng nội bộ cần phải hỗ trợ:

+ Giao thức mạng: IPv4, IPv6

+ Về khả năng hỗ trợ cấu hình đơn giản: 802.1AF, CDP, LLDP, LLDP-MED

+ Về bảo mật: IBNS (802.1X), (CISF): port security, DHCP snooping, DAI, IPSG

+ Định danh: 802.1X, MAB, Web-Auth

+ Dịch vụ kiểm soát mạng thông minh: PVST+, Rapid PVST+, EIGRP, OSPF, DTP, PAgP/LACP, UDLD, FlexLink, Portfast, UplinkFast, BackboneFast, LoopGuard, BPDUGuard, Port Security, RootGuard

+ Các giao thức đảm bảo tính sẵn sàng cao: HSRP, GLBP, VRRP

+ Nguồn điện: PoE

Hạ tầng mạng di động

Sử dụng mạng di động trong trao đổi thông tin, báo cáo

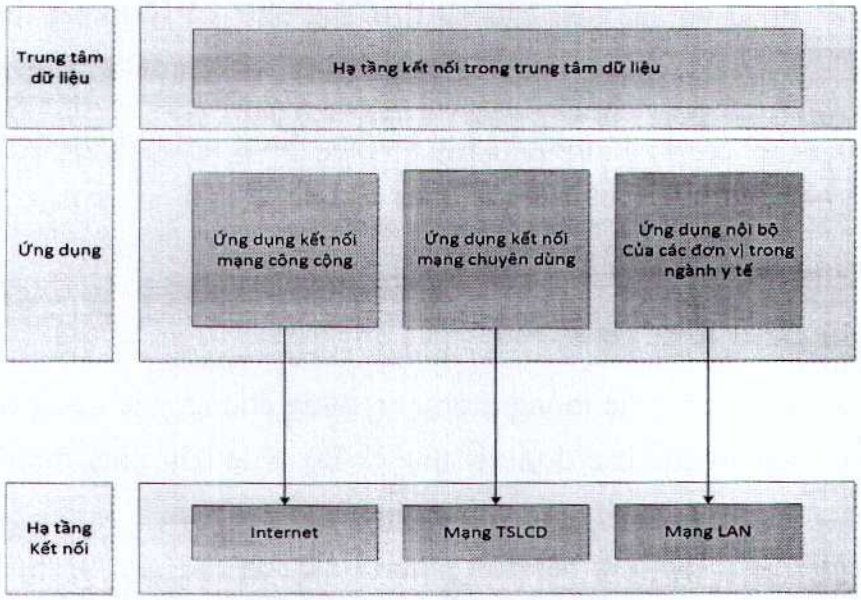
Hạ tầng mạng số liệu chuyên dùng

Sử dụng mạng số liệu chuyên dùng trong trao đổi các hệ thống nội bộ của ngành Y tế

Hạ tầng mạng Internet

Phục vụ cho các ứng dụng kết nối mạng ra bên ngoài

Mô hình tham chiếu hạ tầng truyền dẫn của Bộ Y tế như sau :



c) Hạ tầng lưu trữ

Hạ tầng lưu trữ dạng block

- Phục vụ hạ tầng điện toán đám mây và hạ tầng máy chủ vật lý. Cung cấp tài nguyên cho các ứng dụng truyền thống thông thường, ví dụ như máy chủ ảo, lưu trữ cơ sở dữ liệu nhỏ.
- Xu hướng công nghệ all-flash, lưu trữ bằng chip nhớ gần đây giúp cho hầu hết các thiết bị xây dựng hạ tầng lưu trữ dạng block có khả năng thích nghi với mật độ sử dụng của hạ tầng tính toán, đặc biệt là hạ tầng điện toán đám mây.

Hạ tầng lưu trữ đối tượng (object)

- Phát sinh từ nhu cầu thực tế về dữ liệu hồ sơ y tế , các hình ảnh liên quan.
- Cung cấp dung lượng lưu trữ rất lớn (petabyte, exabyte scales).
- Một trong nhưng lý do để tách biệt giữa hạ tầng lưu trữ dạng block và hạ tầng lưu trữ đối tượng nhằm giảm chi phí và giảm overhead trong việc lưu trữ các dữ liệu khá đặc thù, không cần hiệu suất cao như đã đề cập ở trên.
- Hạ tầng lưu trữ hiệu năng cao
- Phục vụ các yêu cầu rất đặc biệt như xử lý thông tin trong bộ nhớ (in-memory computing) hoặc các workload như CSDL, Data warchouse.
- Bao gồm các thiết bị lưu trữ với dung lượng thấp đến trung bình như có băng thông rất cao và độ trễ rất thấp.

5. Trung tâm dữ liệu Bộ Y tế

Nguyên tắc :

- Tất cả các hệ thống thông tin dùng chung, các hệ thống thông tin chuyên ngành của các đơn vị thuộc Bộ Y tế đều phải được cài đặt, vận hành, khai thác tại Trung tâm dữ liệu của Bộ Y tế.
- Các máy chủ, hệ thống thông tin của các đơn vị thuộc Bộ Y tế sẽ từng bước tập trung, chuyển đổi và đồng bộ lên trung tâm dữ liệu của Bộ Y tế trên nền điện toán đám mây.
- Từng bước hoàn thiện trung tâm dữ liệu của Bộ Y tế ở mức nền tảng như một dịch vụ (Paas : Platform as a Service) cung cấp các APIs cho các đơn vị sử dụng.
- Hoàn thiện trung tâm dữ liệu tập trung của Bộ y tế, từng bước triển khai trung tâm dữ liệu dự phòng của Bộ Y tế.

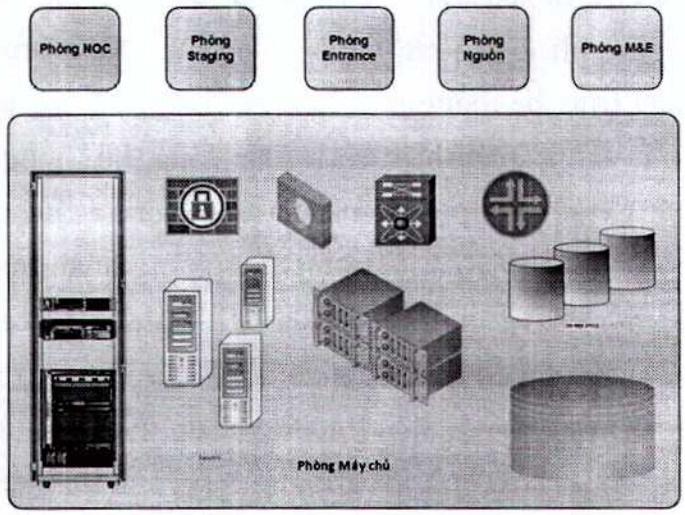
Yêu cầu đối với trung tâm dữ liệu ngành y tế

- Modul hóa để dễ dàng cho việc mở rộng thay đổi cấu trúc hệ thống một cách linh hoạt, thời gian downtime là ngắn nhất có thể.

- Thiết kế theo hình thức module, khả năng mở rộng dễ dàng, các thiết bị được đề xuất trang bị và sử dụng trong Trung tâm dữ liệu không lạc hậu về công nghệ ít nhất trong vòng 5 năm tiếp theo.
- Trung tâm dữ liệu dạng module hoá để tiết kiệm không gian nhưng vẫn đảm bảo các yêu cầu thiết yếu về lưu trữ, truyền tải, xử lý thông tin và cung cấp một Cơ sở vật lý hạ tầng thiết yếu NCPI (Network- Critical Physical Infrastructure) có chất lượng cao đi kèm.
- Thiết kế và xây dựng với đầy đủ các hạng mục/thành phần cơ bản như hệ thống lạnh, hệ thống nguồn điện, hệ thống lưu điện, hệ thống mạng và mạng trục, hệ thống phòng cháy chữa cháy, hệ thống quản trị truy cập vật lý, hệ thống phát hiện rò rỉ chất lỏng, hệ thống sàn nâng, hệ thống máy phát…Các phòng chức năng riêng biệt tối thiểu cần phải có trong DC là phòn máy chủ và thiết bị mạng , phòng quản trị điều hành (NOC), Phòng tiếp đón nhà cung cấp và phòng đệm (Entrance room và Staging room), Phòng nguồn cơ điện và điều hòa (Store house room và UPS room).
- Vận hành với mức tiêu thụ điện năng thấp, thân thiện môi trường với mức tổng chi phí sở hữu (TCO) cho 5 năm là thấp nhất, có khả năng mở rộng lên đến 10 năm
- Căn cứ theo tiêu chuẩn TIA -942 và yêu cầu theo thông tư số 03/2013/TT-BTTTT ngày 22/01/2013 của Bộ Thông tin và Truyền thông quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu việc thiết kế, quản trị thực hiện xây dựng, xây dựng, bàn giao và vận hành Trung tâm dữ liệu của tỉnh sẽ Tier 2+ và hướng tới Tier 3.
- Trung tâm sẽ bao gồm nhà điều hành; hệ thống máy chủ; thiết bị bảo mật; thiết bị mạng và lưu trữ; hệ thống phòng chống cháy nổ và các thiết bị khác bảo đảm yêu cầu về năng lực xử lý, lưu trữ, bảo đảm an toàn dữ liệu lớn, khả năng vận hành 24/7 và đạt các tiêu chuẩn, quy chuẩn kỹ thuật như sau:

  Hạ tầng kỹ thuật viễn thông đạt tiêu chuẩn cấp 2 trở lên theo TCVN 9250:2012 hoặc các tiêu chuẩn tương đương hoặc cao hơn.
- Chống sét cho các trạm viễn thông và mạng cáp ngoại vi viễn thông đạt quy chuẩn kỹ thuật quốc gia QCVN 32:2011/BTTTT.

- Tiếp đất cho các trạm viễn thông đạt quy chuẩn kỹ thuật quốc gia QCVN 9:2010/BTTTT.
- Phương tiện phòng cháy và chữa cháy cho nhà và công trình
- Trang bị, bố trí, kiểm tra, bảo dưỡng đạt tiêu chuẩn quốc gia TCVN 3890:2009 hoặc các tiêu chuẩn tương đương hoặc cao hơn.
- Về an toàn cháy cho nhà và công trình đạt quy chuẩn kỹ thuật quốc gia QCVN 06:2010/BXD.



VI. Kế hoạch thực hiện giai đoạn 2018 – 2020

STT	Nội dung	Năm		
		2018	2019	2020
1	Triển khai cổng thông tin dịch vụ công của Bộ Y tế, tích hợp với các dịch vụ công đã triển khai của Bộ Y tế.			
2	Triển khai, từng bước hoàn thiện hạ tầng kỹ thuật của trung tâm dữ liệu Bộ Y tế; hạ tầng mạng của Bộ Y tế			

STT	Nội dung	Năm		
		2018	2019	2020
3	Từng bước triển khai hệ thống đảm bảo an toàn, an ninh thông tin của Bộ Y tế; xây dựng trung tâm giám sát an toàn, an ninh thông tin ngành Y tế			
4	Xây dựng, triển khai phần mềm hồ sơ sức khỏe điện tử, hệ thống thông tin quản trạm y tế xã, phường, thị trấn;			
5	Xây dựng, triển khai phần mềm thống kê ngành y tế			
6	Xây dựng, triển khai kho dữ liệu y tế quốc gia			