Project submission due date: 5/7/2024, Date submitted: 5/7/2024

Team leader: Nicholas Wharton Signature: Nicholas Wharton

Team members:

Role: On-site Infrastructure (other than APs, VoIP, Network Services, Rack Config), Cloud Infrastructure, Data Privacy (other than data compliance per region), PCI DSS, Site Diagram and Cloud Diagram.

1. **Name: Nicholas Wharton Signature: Nicholas Wharton Date: 5/7/2024**

Role: Rack Configurations, Rack Diagrams, Network Services, Access Point Setup, VoIP Infrastructure, Hardware/Software Selection

2. **Name: Blake Grubbs Signature:** Blake Grubbs **Date: 5/7/2024**

Role: Researcher (VCDPA, Norwegian Privacy Act)

3. **Name: Derek Natali Signature:** Derek Natali **Date: 5/7/2024**

Role: Researcher (Great Britain Data Protection Act, French Data Protection Act)

4. **Name: David Boulos Signature: David Boulos Date: 5/7/2024**

Role: Researcher (HIPAA, Data Protection Act)

5. **Name : Elijah Haynes Signature: Elijah Haynes Date: 5/7/2024**

Role: Researcher (GDPR, CCPA)

6. **Name : Lam Nguyen Signature: Lam Nguyen Date: 5/7/2024**

Creating the Network Infrastructure for a Multi-Site Medical School

Nicholas Wharton, Blake Grubbs, Derek Natali, David Boulos, Elijah Haynes, Lam Nguyen

University of North Texas

CSCE 4535: Introduction to Network Administration

Dr. Ervin Frenzel

Date Issued: 05/07/2024

Table of Contents

Requirements

Hospital Service

The hospital will be a Class C/3 hospital. Meaning that the hospital will only provide day surgeries. Especially since the hospital is an education facility at its core. The focus should be on providing education to the students while also offering them opportunities for learning through lower pressure procedures. Which also is reflected by the amount of patient floors. Only being 2 of the 5 floors. So the hospital will have a limited capacity which is restricted by the bed count of 64. Since each patient floor will have 32 rooms.

Application Requirements

Office 365:

- Microsoft Word - 100 - 150 Kbps
- Microsoft Excel - 150 - 200 Kbps
- Microsoft Powerpoint - 4 - 4.5 Mbps

(ErikjeMS, 2024)

Instructure Canvas: 512 Kbps

Epic - 90 Mbps - 1500 Mbps download speed

(Epic, n.d.)

Ellucian Cloud:

- "Maintain at least 1 Gbps bi-directional data center connectivity to the Public Internet with diverse providers and physical entrances"

(Ellucian Cloud Software Standards, n.d.)

On-Site Infrastructure

VLAN Specifications

Other than the native VLAN, the VLANs will be numbered to identify the site number, floor number, and purpose as seen below. The following example will represent the VLANs for site 1 and floor 1:

- **1** : Management (Native)
- **111**: Computer
- **112**: VoIP
- **113**: Wireless
- **114**: PTR / Files
- **115**: Security (Logs)
- **116**: Medical Devices (x-ray, MRI)
- **117**: Security Cameras
- …
- **119**: Network Devices

The management VLAN, which is the native VLAN, will be used to send device management traffic. This is different from the Networking Device (purpose 9) VLAN which will be the public

facing address for the networking devices. The computer VLAN (purpose 1) will be used for all traffic sent to the physically connected workstations. Which will be trunked along with the VoIP traffic (purpose 2). The VoIP phones will then forward the computer VLAN traffic to the connected workstations. The PTR/Files VLAN (purpose 4) will be used to send all file data between the TFTP server, the printer server and the printers etc. The security VLAN (purpose 5) will be used by the network and security devices to send their syslog traffic to the aggregation servers. The medical devices VLAN (purpose 6) will be logically separated so the traffic can be prioritized as this data will be mission critical. While also the security camera (purpose 7) video data will be logically separated from the other traffic.

It should also be noted that for the outside VLAN the floor will be one value greater than the top floor of the building. So since the sites each have 5 floors, the outside devices will have the floor value of 6 to distinguish it from the other floors. This is because you cannot represent a floor number of 0 in an ip address since the floor is the tens digit of the second octet (as explained in the ip address specifications later in the paper). While also it would be more confusing to set the value as 1 because then all the other floors numbers would not match the number represented.

VLAN Trunking

IEEE 802.1Q trunking will be used to trunk the VLAN traffic over the connections in the site LANs. The examples that follow will use the first site as an example and the VLAN specification as listed above to demonstrate which VLANs will be trunked over which links. For the connections between the MDF switches and the gateway routers the traffic will trunk the VLANs: 1, 111-119, 121-129, 131-139, 141-149, 151-159 and 161-169.

For the connections between the MDF switches and the IDF switches the traffic will trunk the VLANs related to the floor. So for the surgical floor (floor 3) the connections between the MDF switch and the IDF switch will trunk the traffic of the 131-139 VLANs.

There will be additional trunk links to user devices such as the VoIP devices will receive a trunked connection from its associated floors IDF switch containing the VLANs of purpose computer (1) and VoIP (2). Because then the VoIP phones will provide an access link to the connected workstations.

All other user devices will receive an access link from the IDF switch with the VLAN corresponding to their associated site and floor. This includes the wireless APs (purpose 3), printers (purpose 4), medical equipment (monitoring equipment, MRI machine, etc.) (purpose 6) and the security cameras (purpose 7).

Once the trunked traffic reaches the gateway router the VLAN tag (if it isn't the native VLAN) will be stripped to forward the traffic to the CSU/DSU to be sent over the leased line connection. When the response to the traffic returns the gateway router will retag the traffic based on the source IP address of the traffic. This will allow the returning traffic to be sent over the trunked links into the LAN.

IP Address Specifications

The LAN device interfaces will be associated with an inside local address to identify the interfaces for intra-network communications. Each address will utilize the network portion of the address to identify the general location of the device associated with the interface and the purpose if necessary. Which ultimately identifies the VLAN the interface is associated with.

Starting with the devices which are connected to the network via physical media. The first octet will always be set to 10, the second will be set to the site number (1-6), and the third will be set to the floor number (1-6) with the purpose number (1-9) appended to it. With the subnet mask of 255.255.255.0 as the host portion of the addresses are represented by only the last octet.

- The address 10.1.12.34 would represent a VoIP phone at the first site on its first floor.
- The address 10.3.32.123 would represent site 3, floor 3, and purpose 2.

Wireless interface addresses that are associated with an authorized user will fall into a different IP address scheme. This way the wirelessly connected devices will not have the ability to directly interact with the physically connected devices as no routing between the two will be configured. The subnets address will work off the class B private address range. With the network portion of the address represented by the first octet being 172, the second octet being 16-31, the third octet being the site number (1-6) with the floor number appended to it (1-5). Then the last octet would represent the host. Only the site and floor numbers need to be represented since the connection is wireless; it's assumed that its traffic will be wireless VLAN traffic (purpose 3). The subnet mask would be 255.255.255.0 since only the last octet represents the host portion of the address.

- The address 172.16.22.54 would represent a wirelessly connected device at the second site on the second floor.
- The address 172.23.53.12 would represent a device at site 5, on floor 3, with purpose 3.

Lastly is the wireless interface address associated with an unauthenticated guest user. Again we will use a separate IP addressing scheme to separate these devices from all others on the network. The address range will fall into the class C private address range. Where the first octet is set to 192, the second to 168, and the next two octets will represent the host. Because of this the subnet mask for the addresses will be 255.255.0.0.

- The address 192.168.2.24 will represent a guest user on the network.

All of these addressing schemes utilized in tandem will allow for each of these devices to function on the same network infrastructure, without the ability to communicate with each other. This is important as each has a different amount of authorization based on their user role and network requirements.

PAT (NAT Overload)

PAT will allow each campus to have a single or couple of global IP addresses which will be publicly accessible. While not being able to address traffic directly to local site devices. Configuring each client's communications to use a unique port number. This way the communication can be mapped so once the trafficleaves the network its source address is

translated from the inside local to the outside global, which can be mapped back when the response returns. Which allows for the traffic to then be forwarded in the LAN. This provides an extra layer of security as an outsider would have to know the unique port number for the connection to be able to reach the local device.

Gateway Routers

Redundant Gateway routers (Cisco ASR 1002-HX) ensure the network can receive and transmit packets with high availability. The routers will be associated with the same VRRP group and be accessible through the same virtual IP address. They will be configured to function in an Active-Passive configuration. This means one will be the primary router that functions unless it runs into a problem, which is where the routing will be handled by the backup router. Where the VIP represents the active router at the time of its functioning.

These routers will be connected to leased lines for a direct secure connection to the cloud services. All traffic leaving each of the sites will first travel to the cloud infrastructure. Which can then filter the traffic and forward it out to the public internet if necessary. Acting as a proxy server for all traffic that isn't just accessing services on the cloud infrastructure.

Because leased lines are in use a Channel Service Unit/Data Service Unit (CSU/DSU) device is required to translate the WAN signal to be readable by the gateway router. Since the WAN protocol used to send the traffic over the leased lines needs to be converted to the LAN ethernet protocol used by the gateway router and the rest of the devices on the site network. The CSU/DSU would be a separate module that would be installed in each of the Cisco ASR

1002-HX routers. Each of the redundant routers would have a separate leased line connection which would lead to their CSU/DSU module. Which would then convert the traffic to ethernet so the router can forward the traffic into the LAN.

In-line Security Infrastructure

There will be inline next-generation firewalls (Fortinet Fortigate FG-100F). The firewalls are required to drop packets entering or leaving the network based on the configured policies. While also able to scan the payload data of the packets for malicious data. Because these devices are inline they will be required to be redundant. Since on their own, their failure would stop all traffic from reaching or leaving the network. Both of the NG firewalls will be connected to both of the gateway routers and both of the MDF switches. Though they will not be used at the same time. One of the NG Firewalls will be the primary and the second will be a failover secondary firewall. This will utilize VRRP similarly to the gateway routers to provide the NG Firewalls with a virtual IP which will be used to make routing to the NG firewalls simple as the other devices will not have to know which Firewall is running.

The next-generation firewalls contain multiple blades which must be configured in the correct order, these blades are as follows: encryption, URL filtering, IPS, antivirus and spyware. Ordering in this context represents when in the process of receiving traffic that each of these processing actions take place. Firstly all packets forwarded to the next-generation firewall will have their payloads encrypted. So the firewall first must compare the packet headers with the packet filtering policies configured. If the packet should be dropped based on its source device for instance it can decrease the unnecessary processing by dropping the traffic before it deals

with any of the other blades. If the packet remains then the payload needs to be decrypted (with a key dependent on the source of the packet). From this point, the IPS, antivirus, and spyware scanning can occur simultaneously. Once this processing is complete the packet payload can be encrypted based on the destination of the packet to be forwarded to said destination. The NG Firewalls will be configured to function in transparent mode so it will inspect the packets then forward the data to the MDF switch if not dropped. Since there is no need for the NG Firewall to make routing decisions.

Additionally, an out-of-band IDS will be connected to the distribution switches. The distribution switches will be configured to mirror their uplink ports to copy the data to the IDS system. Then all of the packet data can be run through the IDS for further network traffic analysis. Having the device out of band means that it will not interrupt the routing of traffic on the failure of the device. Since it's not as time-sensitive for the IDS to get the traffic data, since it already ran though the IPS. The IDS is for further processing and analysis post the traffic entering the network.

Connected between the MDF and IDF switches are Data Loss Prevention (DLP) devices which will scan all of the packet data leaving the floors. This is done to prevent a DLP device placed between NG firewall and MDF switches from being the bottleneck of all outgoing traffic in the network. While still providing the DLP services to all of the traffic that leaves the network.

MDF and IDF Rack Configurations

The MDF rack hardware will include two 48 port 2U patch panels, a 1U tape backup, two 96 port Cisco N9K-C93360YC-FX2 switches, two Fortinet Fortigate FG-100F next generation firewalls, four VMWare servers and two UPSs. These will be connected to two Cisco ASR 1002-HX gateway routers with two individual 40Gb ethernet connections converted by the CSU/DSU from the two individual leased line connections. The connection from these routers will enter the Fortinet NGFWs then exit to the switches which will be connected to the 2 UPSs, 4 VMware servers, Tape Backup and the IDF on the same floor and the floor above it. This ensures availability through redundancy as if any component fails the system will still function.

The IDF cabinets will be configured with two 48 port 2U patch panels, four 48 port Cisco Catalyst 9300X-48HXs, a DLP device and two UPSs. The Cisco Catalyst 9300X-48HXs ensure that any devices that require POE such as the VoIP phones and CCTV cameras will receive power.

Both the MDF and IDFs will have two PDUs running up the sides of the rack, one connected to each UPS, to provide redundant power to each device on the rack that supports it. The cabling on the racks will be color coded as such, lease lines to routers will be black, routers to NGFWs will be red, security devices to switches or switches to security devices will be yellow, switches to servers will be blue and UPSs to switches will be gray.

Switching Infrastructure

An MDF rack will be placed on the first floor in a central location for easy access and to minimize the risk of the MDF rack flooding. Then the MDF switches will be connected to five IDF cabinets which will be placed on each floor. This is done firstly to reduce the amount of distance required for the connection between the switch and the end devices. Additionally, it further compartmentalizes the network as only the VLAN traffic associated with the specific floor will be accessible at each of the IDF cabinets.

Both the MDF and IDF switches need to be able to handle VLAN trunking. Especially for the MDF switch which will be required to trunk the native VLAN along with the other 8-purpose VLANs to each floor's IDF switch. But also the IDF switches that need to receive this trunked traffic and provide trunked traffic to the VoIP phones which will forward the physically connected workstations traffic. Additionally, the IDF switches will be required to provide POE since they will have to power the VoIP phones, the wireless APs, and CCTV cameras for each floor.

CCTV Cameras

There will be 72 interior CCTV cameras and 32 exterior CCTV cameras located on the hospital's premises. With 12 CCTV cameras on each of the 5 floors, and an additional 12 for the basement. The CCTV traffic will have its own VLAN designated for each floor. The CCTV cameras will be powered via POE 802.3bt to reduce the amount of power cabling required for implementation. Which also extends the possible locations where the cameras can be placed. The indoor cameras

will be placed only in hallways, staircases, elevators, and near exits to give patients privacy inside the clinic, and patient rooms.

Each site will store the site's CCTV footage in a centralized storage. Which will be a file storage server which is connected to the MDF switches. This way all of the footage can be easily accessible when needed, while also not wasting cloud resources constantly transmitting the footage to stores outside of the campus. It's also unnecessary to have it in the cloud as no other site would need to access another site's CCTV footage.

Optiview has outlined that, “We would recommend using the ‘3MP at 20fps’ setting” (*CCTV camera resolution: CCTV Resolution Chart for cameras* 2022) But to reduce storage requirements with the large amount of cameras that have to be taken into account, 2MP at 15fps would work fine. Especially since this would remain an HD video before compression. With 24 hours of constant recording, with 2MP at 15fps, each camera would use:

- Frame Size = 1920 * 1080 * (3 * 8) = 6.2208 MB
- Number of Frames = 24 hrs * 60 mins * 60 secs * 15 fps = 1,296,000 frames
- File Size = 6.2208 MB * 1,296,000 frames = 7.68 TB
- For 104 Cameras = 7.68 TB * 104 = 798.72 TB of raw footage per day

But this video would be compressed before being sent to the centralized storage. Though it is difficult to estimate the amount of compression that would occur. Since the amount of compression depends on the variability of the video, motion, colors, etc. It would be fair to say

that using H.265 compression for instance would heavily reduce the amount of storage required. Especially since the goal of the storage would be to have the footage last for 30 days before it can be rolled over with new footage. A possible estimate calculated using Seagates surveillance storage calculator under the conditions of 104 cameras, H.265 compression, 1080p, 15 fps, 24 hours of footage per day, to be stored for 30 days, with a medium quality video compression setting would set the "required storage space 50.54 TB" (*Surveillance storage calculator: Seagate US*) Which is a reasonable amount of footage to store especially in comparison to the nearly 800 TB of raw footage per day, which would be 24000 TB per month. So the centralized storage should amount to around 100 TB of storage to be able to handle the temporary storage of the previous 30 days compressed CCTV footage.

VoIP Infrastructure

We plan to use Cisco 8811 IP Phones and power them with POE 802.3at from the IDF switches on their respective floors. The VoIP phone management software will be 3CX and will run off of the VMs in the MDF.

Network Services

The network services such as DHCP, TFTP, NTP, SCCM imaging, Syslog aggregation, BootP, VoIP phone service, printer service, video management service and EMR service will be virtualized and run off the VMWare ESXi servers in the MDF rack. Milestone XProtect will be utilized as the video management software, Cisco Unity will be utilized for the VoIP phone service, Windows Print Server will be utilized for the printer service and EPIC will be utilized

for the electronic medical records (EMR). This will allow for centralized and remote management of all of the services. Each of the services software will be hosted on at least two of the physical servers. Allowing for redundancy for DHCP for instance in case one of the physical servers goes dark it won't be the only one providing DHCP configuration information to the devices.

The NTP server will pull from the azure cloud Stratum 1 NTP server which is synchronized with all of the azure cloud regions. This way each of the sites will have nearly the same time. Which is important mostly for the logging, but for other mechanisms. The site NTP servers will then be accessed by the networking devices and security devices on the network. The NTP server will be an Azure VM running on the VMware servers connected to the MDF switch to provide each site with a local Stratum 2 NTP server.

Network Configuration Settings

Both DHCP and BootP will be required to provide the basic network configuration settings to devices on a per-site basis. Though I am combining these two services together here since they are similar, “Remember that you can’t run BOOTP and DHCP servers simultaneously on the same system, because both servers use the same ports.” (*BOOTP, DHCP, and Network Computers: Your Absolute Best Practices* 1999) However, this will not be a problem as the VoIP VLAN and the wireless VLAN are logically separated. Allowing for the different services to run concurrently without colliding.

DHCP pools will need to be defined for each of the wireless VLANs for each floor of each site. Since these wireless devices are those which will need to be connected and disconnected constantly. Thereby accessing their network configuration settings dynamically. Which would help to not bog down the users. However, outside of these wireless devices, the rest of the devices on the network (network and security devices, physically connected workstations, and medical devices) would make more sense to have static network configurations. Since they will need to be accessible, so dynamic assignments would make this difficult. In addition to the IP pool the DHCP server should be configured to point the devices in the direction of the cloud DNS server, the address of the default gateway, and the address of the wireless LAN controller.

BootP will be configured with the manual mappings of the VoIP phone's MAC address to their assigned IP address. In addition to providing the devices with the address of the gateway router, and the address of the TFTP server. The TFTP server is necessary to provide each of the VoIP phones with their boot instructions.

Exchange Server

The Microsoft Exchange Server will be the arbiter of all Office 365 data generated by the O365 accounts linked to the school. So all forms of communication such as email, calendars, messaging/video calls through teams, in addition to cloud file storage such as SharePoint are just the major pieces. This O365 traffic will initially run through the local sites Exchange server. Where the O365 data will be stored. Then every 30 minutes the O365 data will be synchronized with the microsoft cloud.

Since as noted in the Microsoft compliance offerings, “Microsoft enables customers in their compliance with HIPAA and the HITECH Act and adheres to the Security Rule requirements of HIPAA in its capacity as a business associate.” (Health Insurance Portability and accountability act (HIPAA) & health information technology for economic and clinical health (HITECH) act - microsoft compliance 2024) While the article (Microsoft Compliance Offerings) further details how the microsoft exchange server, and the microsoft cloud comply with the regional legislations such as the GFPR, CCPA, and VCDPA. So having the data stored in the microsoft cloud takes some of the pressure off of the IT admins as they will not have to deal with compliance in regards to the archived exchange data.

Though the information will be synchronized with the microsoft cloud, the site exchange server will retain the sites exchange data for 30 days. Allowing the recent and active O365 data to be accessed with low latency. If the site loses connection to the outside, communications will still persist within the sites.

EMI Interference Considerations

Electromagnetic Interference “can cause excessive retransmission of data, lowering the effectiveness of the network. Worse, though, is the possibility of EMI causing errors in medical equipment, leading to faulty readings, missed diagnoses, or malfunction in treatment equipment.” (*Designing a reliable cabling infrastructure for healthcare facilities* 2010) Shielded twisted pair connections will be required for the radiology room in the clinic. MRI machines emit a static magnetic field, “The SMF is always on regardless of whether the scanner is active or not. The flux density used in MRI scanners is typically 1.5 or 3 T” (Frankel, 2018) For the

same reason the MRI room needs to be a Faraday cage. Both to reduce the exposure of all people to EMI, but also to reduce the chance that the pacemaker of a patient visiting the clinic doesn't get interfered with. The MRI machine room should additionally be placed in a sectioned-off area that warns of possible interference. Also, no patient room should be placed directly over or under the MRI room.

Now for the heart clinic, it will be necessary to use shielded twisted pair cabling to reduce the chance of the cabling interfering with the pacemakers of patients. While also applying EM reflective shielding around the room to further extend these protections. This extends to the pharmacy of the hospital which will be distributing medical equipment such as pacemakers. For this reason, all connections in the pharmacy need to be shielded, and the room needs to have EM reflective shielding surrounding the room. However, a patient with a pacemaker may require non-heart-based treatment or may need to stay in a patient room. For this reason, there needs to be designated clinics and patient rooms with EM reflective shielding to further protect these patients.

Access Points

The access points (Cisco Catalyst 9136) will be connected to the Cisco Catalyst 9300X-48HXs in the IDFs on their respective floors. Each AP will be staggered with the ones on the floors above and below it to provide full coverage. The WAPs will be configured as a mesh network with redundant wireless access controllers run off of VMs on the VM servers in the IDFs on their respective floors. The WAC software that will run off of the VMs will be Cisco Virtual Wireless Controller (vWLC). They will be powered using power over ethernet 802.3bt (POE). This allows

for the access points to be positioned anywhere that the network cables from the switches can reach. Without the need to have additional planning for powering the device with a separate power source. These APs operate on the 2.4 GHz, 5GHz and 6GHz bands simultaneously and will be connected to two separate switches in the IDFs on their respective floors for redundancy.

To be authorized access to the wireless network, users will have to be authenticated by the cloud AAA server. Where the user will be prompted to input their username and password. Which will be followed by a second layer of authentication based on the user's configured MFA settings. Once authenticated the user will be authorized to access network resources based on their account role and the site they are connecting from.

Clinical Floor Infrastructure (Floor 1)

The clinical floor will include 11 clinic rooms, and the MRI room. This floor will require the connections necessary for the medical equipment such as the MRI machine. While the medical staff will require their own equipment such as their own VoIP phones which also forward the traffic of a connected workstation. With equipment such as a printer. While also having the wireless APs covering the floor. This will allow for any extra devices from the staff and visitors to connect to the network either through their account or as a guest. There will also be 12 CCTVcameras distributed around the floor. All of the devices on the floor will connect to one of four Cisco Catalyst 9300X-48HX switches. Where all of the devices will have a single connection to one of the first three switches. Then the fourth will provide the critical devices redundancy. The dual-NIC devices such as wireless APs and the medical equipment such as the

MRI machine will have an additional connection to the redundant switch. While also the switch will provide power through POE to the security cameras and the wireless APs.

Surgical Floor Infrastructure (Floor 2)

The surgical floor will include 12 surgical rooms. This floor will require the connections necessary for the medical equipment such as the Operating room telephony, and other equipment. While the medical staff will require their own equipment such as their own VoIP phones which also forward the traffic of a connected workstation. With equipment such as a printer. While also having the wireless APs covering the floor. This will allow for any extra devices from the staff and visitors to connect to the network either through their account or as a guest. There will also be 12 CCTV cameras distributed around the floor. All of the devices on the floor will connect to one of four Cisco Catalyst 9300X-48HX switches. Where all of the devices will have a single connection to one of the first three switches. Then the fourth will provide the critical devices redundancy. The dual-NIC devices such as wireless APs and the medical equipment such as the OR equipment will have an additional connection to the redundant switch. While also the switch will provide power through POE to the security cameras and the wireless APs.

Patient Floor Infrastructure (Floors 3 and 4)

The patient floors will include 32 patient rooms surrounding a central area for the nurses and doctors. The patient rooms themselves will require the connectivity of 1 VoIP phone each, while also requiring the connections necessary for the medical equipment such as the monitoring

equipment. While the medical staff will require their own equipment such as their own VoIP phones which also forward the traffic of a connected workstation. With equipment such as a printer. While also having the wireless APs covering the floor. This will allow for any extra devices from the staff and patients to connect to the network either through their account or as a guest. There will also be 12 CCTV cameras distributed around the floor. All of the devices on the floor will connect to one of four Cisco Catalyst 9300X-48HX switches. Where all of the devices will have a single connection to one of the first three switches. Then the fourth will provide the critical devices redundancy. The dual-NIC devices such as wireless APs and the medical equipment such as the monitoring equipment will have an additional connection to the redundant switch. While also the switch will provide power through POE to the security cameras and the wireless APs.

Educational Infrastructure (Floor 5)

The educational staff will require their own equipment such as their own VoIP phones which also forward the traffic of a connected workstation. Which would then be connected to projectors and speakers for classroom presentations. With equipment such as a printer if required. While also having the wireless APs covering the floor. This will allow for any extra devices from the staff and students to connect to the network either through their account or as a guest. There will also be 12 CCTV cameras distributed around the floor. All of the devices on the floor will connect to one of four Cisco Catalyst 9300X-48HX switches. Where all of the devices will have a single connection to one of the first three switches. Then the fourth will provide the critical devices redundancy. The dual-NIC devices such as wireless APs will have an additional connection to

the redundant switch. While also the switch will provide power through POE to the security cameras and the wireless APs.

Outside Infrastructure (Labeled as Floor 6)

The outside infrastructure would be set up to provide connectivity to the security cameras placed around the perimeter of the site. The rack would be configured exactly as the other IDF racks. Containing 4 Cisco Catalyst 9300X-48HX switches so the amount of cameras can be expanded on or other devices can be added in the future. While also the switch will provide power through POE to the security cameras. The diesel generators for powering the hospital if the power grid fails would also be located around this area.

Logging

Logging will take place for all network and security devices of each site. The logging data from each of these devices will be forwarded to a syslog aggregation server connected to the MDF switch of each site. This local aggregation server will then normalize the logging data for each site before forwarding the site's log data to the centralized cloud-based logging aggregation server. This is additionally where the cloud Oracle database will directly deliver its database access logs. Which will collect the logging traffic from all of the sites and normalize the multisite logs. This is accomplished by utilizing coordinated universal time (UTC) so all of the logs coming from different regions of the world will be contextualized to the same representation of time.

The normalization process that takes place at the MDF connected aggregation server, and at the cloud aggregation server will follow 4 steps. These steps are as follows 1NF, 2NF, 3NF, and 4NF. The logs when normalized are placed in the 4th normal form which indicates that “As commonly defined, most normal forms include a requirement that earlier normal forms are also met. Therefore, any database that is in 4NF is necessarily also in 1NF, 2NF, 3NF” (Painter‑Wakefield, 2024)

Starting with 1NF, this requires that each record parameter has only one value associated with it and that each record is unique. 2nd normalization form requires, “there are no *non-key attributes* which are functionally dependent on a proper subset of the key” (Painter‑Wakefield, 2024) For instance if there are two records each with the same primary key value, with a single non-key parameter with each record having differing values would make the table not in 2NF.

3rd normalization form requires “there are no non-key attributes which are functionally dependent on other non-key attributes” (Painter‑Wakefield, 2024) If I had a table with a primary key and two non-key attributes, where the first non-key attribute is dependant on the primary key, and the second is dependant on the other non-key attribute. This would not be in 3NF. It would require creating two tables: one where the original primary key is associated with the original first non-key attribute, and a second where the original first non-key attribute is made the primary key and associated with the original second non-key attribute.

Lastly, 4th normalization form requires, “for every non-trivial multivalued dependency of the form $X \twoheadrightarrow Y$ on the relation, X is a superkey of the relation.” (Painter‑Wakefield, 2024) For

example, if you have a primary key that represents an individual and two non-key attributes that are not related to each other. Let's say the non-key attributes are favorite foods and colors. If an individual is related to one food and two colors it would require two records to demonstrate both of the colors. So both of these records would have the one food as the parameter for both records. This would need to be split up into two tables each with the primary key that represents the individual, and each with a single non-key attribute of either the food or color. Since the relationship between the two non-key attributes is trivial, it makes the data more integral to represent these isolated relationships on their own.

Once the syslog data is aggregated and normalized in the centralized cloud syslog server. This data will be passed to the SIEM tools to analyze and process the data. As described here, “A defining function of a SIEM is to correlate events to find larger incidents ... This includes the ability to define correlation rules, as well as present the results via a dashboard.” (Knapp & Langill, 2015) The SIEM provides the ability to get a higher-level analysis of the logging data without the need for an administrator to dive head-first into the raw logging data. This then provides the administrator a direction to start in for their incident response, rather than searching through these large pools of data blindly.

NTP monitoring will be conducted through syslog. Where the on site Azure VMs running the NTP server will log important events such as whether synchronization events succeed or fail, if the clock is adjusted, or if an anomaly occurs. This way NTP monitoring can occur, while only sending the logging data when needed, rather than archiving the times of the cloud and site NTP servers and having to analyze the data post mortem.

Users' access of the Microsoft server AD accounts will be logged in the admin log. This will be configured by default. Though it will need to be configured to send the log data to the oracle database. This way all of the log data for all of the sites will have a centralized storage. Though the logs per each site would need to be logically separated by tables.

Network Cabling

Every connection on every site will use shielded twisted pair cabling. For the connections between the CSU/DSU, the gateway routers, the NG firewalls and the MDF uplinks would need to be Cat 8 connections. In addition the Cat 8 connections will be required for the connection between the IDF uplinks and the MDF downlinks. To connect each of the vmware servers to the MDF switches a Cat 8 connection should be used. Additionally to connect each of the MDF servers to the IDF switches a Cat 8 connection should be used.

To connect each of the APs a Cat 7 connection from the IDF switches will be used to provide POE and data to each. This is because for the Cisco Catalyst 9136 AP, “All speeds are supported on Category 5e cabling, as well as 10GBASE-T (IEEE 802.3bz) cabling” (*Cisco Catalyst 9136 Series Access Points Data Sheet* 2024).

A Cat 6 connection will be required for the other POE devices such as the video cameras, VoIP phones, etc. Including the connection to the workstations from the VoIP phones. The physically connected medical devices such as the monitoring equipment and the MRI machine should have Cat 6 connections for each of their interfaces to their corresponding floors IDF switches. While

the rest of the devices such as the printers which require a physical connection should receive a Cat 5e connection to its corresponding floors IDF switch.

Site Personnel

Each site will require three network technicians per site. This way the infrastructure can be managed around the clock to ensure the availability of the network. While also making sure the network infrastructure falls into compliance with the security policies laid out both for the site and the overall campus system that are laid out by the security team. There will also be required a Security Technician for each site who will be incharge of interacting with the security team (all of the security technicians between all of the campuses). To come together and determine the security policies that must be followed. While also being in charge of making changes to the security infrastructure of the network, either delegating the work to a network technician, or to perform the configuration changes themselves.

Cloud Infrastructure

Azure Cloud

The Azure cloud infrastructure will contain most of the publicly accessible servers. This includes the school's web server, exchange server, AAA server, and the school systems Oracle Database. The Azure cloud will also provide third-party access to the Oracle database for its payment, and insurance service providers. While also functioning as a proxy, forwarding traffic from the sites to either the third-party certificate authority or the wider public internet.

Cloud Regions

The Azure cloud has regions that designate the physical cloud infrastructure which will be utilized to host the servers and applications. So multiple regions will be required to provide low-latency access to the cloud servers, and databases for all of the campuses. This can function by utilizing Azure's cross-region replication feature which allows for the synchronization of both the servers and databases between the different regions. This way the users can connect to their local regional cloud service, and in the background, the cloud service will be synchronizing the data between sites.

Public Internet Access

The cloud will act as a proxy server for all public internet traffic leaving the sites. Because of this, the only external connection to each site required is the leased line to the cloud infrastructure. Which allows for the cloud infrastructure to apply URL filtering and WAF

policies on the traffic. So it can make this decision based on policies set for all of the sites. While also adding minimal latency to this traffic as each site will be connecting to a local regional instance of the cloud infrastructure.

DNS

All DNS requests will be run through a centralized DNS server in the Azure cloud infrastructure. This decreases the amount of DNS management as it will only need to be configured once for all of the sites. Also, all of the sites will have access to the same cached DNS information. If the DNS does not contain the record requested by the user the server will forward the traffic to the authoritative root VeriSign server addresses as 64.6.64.6. This way the majority of DNS requests will be met with the cloud DNS's cache as most of the traffic from the school will be accessing the campus web server, Canvas, Epic, etc. Then if needed a longer recursive request can be made for less requested domain name translations.

AAA and User Access

The authoritative authentication, authorization, and accounting server will be hosted on the cloud infrastructure. This way users' access to local services and cloud services will be handled in tandem. The use of user roles which will be assigned by administrators will decide the user's ability to access resources on the network. The ability for a user to authenticate themselves will be handled primarily through a username and password pair. When a new student of the facility requires a new user account it will be created with a standardized username and temporary password which will be used by the user to initialize their account and configure their password.

However, this won't be the only form of authentication as multi-factor authentication will be required. So the user will be asked to configure an email address, phone number, or push notification application. This will give the user two ways to identify themselves which makes having the user's password exposed less of an issue as the attacker would also need access to the MFA method.

The authentication server will be a Kerberos server. The server will authenticate a user as stated above utilizing the username-password pair which will be compared to the records in the windows server active directory server. If a user object corresponds with the given username and password pair, MFA will be directed based on the configured MFA settings linked to the user object. Then once the user confirms their identity with their MFA method the user will be granted a time-based authorization token to access the network and applications.

NTP

The time will be synchronized through the pre-synchronized stratum 1 devices owned by microsoft. As stated in the azure learn documentation, “Azure hosts are synchronized to internal Microsoft time servers that take their time from Microsoft-owned Stratum 1 devices” (Time Sync for windows VMS in Azure - Azure Virtual Machines 2022) Because of this a azure VM will be required to run on the VMware servers connected to the MDF switches of each site. This way each site can pull the synchronized time from the cloud infrastructure, each having their own Stratum 2 servers. This makes dealing with NTP nearly seamless since the biggest problem

would be synchronization between sites, so having Microsoft take care of this problem makes the NTP configuration much simpler.

Data Privacy

Data Lifecycle

The data will be collected at the campus locations whether from engagement in the educational institution, from visiting the medical facility as a patient, or through employment at the campus. At these junctures, records will be collected and input into the system including (SPI) sensitive private information, (PHI) protected health information, and (PCI) Payment Card Industry information.

Data Warehouse

The data to be stored in the system will be structured. The most important data that will need to be stored includes patient medical data, patient billing data, student billing data, student academic records, medical staff personal information, and teaching staff personal information. These all would be configured as records organized in predefined formats in tables.

Certificate-Based Encryption

For most LAN communications, and between the sites and the cloud infrastructure certificate-based encryption will be used to secure the traveling data. However, it will not be used for instances when a device new to the network has to query the third-party certificate authority for the certificates to be able to communicate with CBE.

The application data will be encrypted using CBE for internal communications, such as SMB communications. Each device will have a private and public key, and the certificates will hold each device's public key. Then when communication occurs the devices will use the authenticated public keys to know their traffic can be read by the destined device.

However, this gets more complicated when being used for communications between the site and the cloud. A device on the site that needs to send traffic to the cloud will first encrypt its traffic payloads with the public key related to the NG firewall of the LAN. Once the traffic reaches the NG firewall the traffic will need to be filtered, and scanned for IPS processing. Then the data will be reentered with the public key of the NG firewall equivalent for the Azure cloud infrastructure (whatever device is used for processing the traffic that enters the cloud infrastructure). Then the cloud will be able to handle the traffic from there.

Then, it's the same process in reverse for data traveling from the cloud infrastructure to the site. Before traffic leaves the cloud network, the payloads need to be encrypted with the public key from the certificate associated with the NG firewall of the site where the traffic can be filtered, and processed. Before being encrypted with the public key of the destined device so only it can read the contents of the traffic.

Devices new to the network will need to gain a certificate to communicate in the network properly. The certificate would be issued to the device when the user authenticates themselves to the network and gains their SSO time-based token. At this point, the device would generate a key

pair and share the public key which would be forwarded to the third-party certificate authority to create the certificate to be shared with the other devices on the network when requested.

Key Storage

The keys for data at rest will be stored on the Azure Cloud Infrastructure in an application different from the Oracle Database where the encrypted resting data is stored. This way if an adversary gets access to the database they can not get access to the data without additionally breaking into the key storage.

While the encryption keys used for data in motion will be generated, initially shared, authenticated and for the public keys available from the third party certificate authority.

Rule and Role-based Authorization

Though all of the site data will be linked to the same database, access to this data should be based on the set rules and role of the user. The rule is the site that the user is accessing the data from. Users related to a specific site should only have access to the data related to their site. While also the role of the user should control what data they can interact with. This implementation will give the system a virtual barrier between each site. While also allowing for further separation at the site level between the users of different roles. The role access is as follows:

- Admin

    - Will have access to all of the data on the network
- Medical Instructor
    - Communication data linked to their instructor account (mailbox, O365)
    - Canvas data linked to their instructor account
    - Ellucian data linked to their instructor account
    - Student data linked to their instructor account
    - EPIC data linked to their instructor account
- Non-Medical Instructor
    - Communication data linked to their instructor account (mailbox, O365)
    - Canvas data linked to their instructor account
    - Ellucian data linked to their instructor account
    - Student data linked to their instructor account
- Student
    - Communication data linked to their student account (mailbox, O365)
    - Canvas data linked to their student account
    - Their Student Record data linked to their student account
- Support Staff (nurses)
    - Communication data linked to their instructor account (mailbox, O365)
    - EPIC data linked to their instructor account

This is in accordance with the implementation of both Biba and Bell-Lapadula concurrently. The Biba model represents, "'no read down' and 'no write up'—guard against the corruption or loss of integrity" (Philpott & Gantz, 2013) While on the other hand, the Bell-Lapadula model

represents, “‘no read up’ and ‘no write down,’” (Andress, 2011) While these policies cannot be explicitly followed they can be morphed to meet the situation of this campus. This means that the user based on their role should only have explicit access to the data as listed above.

Data at Rest

Data in the Oracle Database must be stored securely as the tables will contain (SPI) sensitive private information, (PHI) protected health information, and (PCI) Payment Card Industry information. This would include encryption for the data at rest, with the encryption keys being securely stored separately from the database in a centralized key store hosted on the Azure cloud infrastructure.

For SPI, healthcare data, and payment card data column-based encryption should be used. For example, for patient records the key used to encrypt all of the patient's SSN should be encrypted with a different key than their date of birth. This way if an adversary gets one key they wouldn't have access to all of the information in the table. For non-sensitive data stored in the database, a single key should be used to give a layer of security without the need for it to be as complex as the protections granted to SPI.

Data in Transit

When an authorized user requests data from the Oracle database, the data should be decrypted from its resting encryption using the appropriate key from the cloud-hosted centralized key store. The data will be sent over a leased line connection from the cloud to the site, which offers little

ability for anyone to capture the data. But since the information is sensitive it's necessary to add a layer of encryption to all data passing through the wire. For this reason, certificate-based encryption will be used to get the public key of the processing device for the site network. Then the data can be decrypted by the site processing device which would be the next-generation firewall which will run its packet filtering policies over the data before decrypting the payload to process the payload data (Antivirus, IPS). At this point, if the firewall doesn't decide to drop the traffic it will be encrypted using the public key associated with the certificate of the destination node so it can be securely sent through the LAN network. Where then the destined device can access the data with its private key.

This process for data/requests leaving the site is the same just with the order flipped around. So a device in one of the sites will create traffic to be sent to the cloud. These packets will initially have their payload encrypted using the public key from the certificate associated with the DLP device connected to their floor IDF switch. This way the DLP device can decrypt the payload and run the DLP processing over the data. Then the DLP device will encrypt the payload using the public key from the certificate associated with the next-gen firewall in line with the gateway router before being forwarded to the firewall device. The firewall will run its packet filtering policies on the packet. Then if it's not dropped the packet's payload will be decrypted and processed (Antivirus, IPS). The firewall will then encrypt the packet payload using the public key from the certificate of the processing device for the cloud. Then it will forward the packet to the gateway router which will perform the PAT operations on the packet header and forward the packet to the cloud. Where then the processing device from the cloud will use its private key to

get the payload data and run its security checks on the packet similar to the firewall of the site. Then the data/request will be forwarded to the database to be handled.

Override Access

Override access should be granted to a shortlist of authorized personnel to trump the normal security procedures in the case of an emergency where the data is required immediately. However, this needs to be provided to a minimal number of administrators to reduce the risk of the ability being abused. Doctors employed at the medical facility of the campuses should be able to provide this override access to patient data to emergency responders who require the patient's data. This override access should only be used for patient medical information as there will never be an emergency where the academic or billing information of a student, patient, or employee of the facility would be required. Override access will additionally be required by the IT team (system administrators) to provide maintenance and troubleshooting for the system.

Data Compliance Per Region

Data Protection Act 2018/GDPR for Great Britain

Data protection regulations in Great Britain are governed by the Data Protection Act of 2018, which is supplemented by the United Kingdom General Data Protection Regulation. Part 1 of the Act is subject to the GDPR. The law regulates the processing, collection, and storage of personal data to protect individual privacy *(Data Protection Act 2018)*. Individuals have the right to obtain information concerning the processing of their personal data. If data appears inaccurate,

individuals are able to request the rectification of the data. The Information Commissioner's Office is responsible for monitoring and enforcement of GDPR provisions and the DPA. They must consider the importance of security at appropriate levels for personal data, including the interests of data subjects, data controllers, stakeholders, and general public interest. Part 2 of the Act includes supplementations to the GDPR which must also be compliant with the processing of user data *(Data Protection Act 2018)*. Individuals are able to request access to personal data held by organizations, the right to request removal of personal data once the collected data is no longer necessary for its collected purpose, the right to request restrictions of personal data processing where organizations can store data but not process until all restrictions are lifted, the right to receive a copy of their personal data, the right to request data to be moved to a different data controller, and the right to object automated decision-making processes *(Data Protection Act 2018)*. Part 3 of the Act addresses the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive *(Data Protection Act 2018)*. All personal data used for law enforcement purposes must be processed lawfully and fairly, and be processed for specified, explicit, and legitimate purposes for law enforcement *(Data Protection Act 2018)*. Only the minimum amount of personal data necessary for law enforcement should be processed. Personal data used by law enforcement must be accurate and current, and individuals are still able to request access, rectification, deletion, and restriction of their data, as stated in Part 2. Part 4 of the Act focuses on the regulation of personal data processing by intelligence services *(Data Protection Act 2018)*. Part 5 of the Act focuses on the functions of the Information Commissioner's Office, who is responsible for the overseeing of data protection as described in Part 1 of the DPA *(Data Protection Act 2018)*. Organizations are to ensure IT infrastructures include implementation of data protection measures and respondence

to data subject requests, as set by the ICO. All data breaches are to be reported to the ICO and affected individuals. If not complied, the ICO is able to take action against organizations that violate data protection laws. Part 6 of the Act establishes the enforcement of data protection legislation *(Data Protection Act 2018)*. This includes IT infrastructures that must ensure compliance with data protection legislation, be able to provide access to relevant data during investigations and audits, respondence to data breaches, and corrective measures to address defective data protection practices. The final section of the Act, Part 7, covers supplementary provisions in relation to the Crown and Parliament *(Data Protection Act 2018)*.

Data Protection Act 2018/GDPR for Norway

Norwegian data protection is governed by the Law on the Processing of Personal Data (Personal Data Act) of June 15, 2018, which implements GDPR (*Norway - Data Protection Overview* 2024). This act protects the privacy of the norwegian citizens and individuals residing in norway and contains the number of provisions and requirements related to the processing of personal data(*Norway - Data Protection Overview* 2024). There are multiple applications where both GDPR and the data protection do not apply. Case 1, When it is stated in another law. Case 2,When the processing of personal data is done under the same household. Case 3, for cases that are brought before certain resolutions bodies as set out in Section 2b of the act(*Norway - Data Protection Overview* 2024). The lawful basis where processing personal data is permitted under the following: Data collected by businesses prior to this act, freely given data by the owner, unambiguous consent of the data subject, data that is contractual necessity(*Norway - Data Protection Overview* 2024). Data in compliance with legal obligations, explicit consent of the affected data subject, employment law, if your processing is necessary for the establishment,

exercise or defense of legal claims, or for legitimate interests(*Norway - Data Protection Overview* 2024). There is a Norwegian Data Protection Authority that operates as Datatilsynet. Datatilsynet is an independent supervisory authority that is financed by the government of Norway itself stated in section (20) of the act itself(*Norway - Data Protection Overview* 2024). Datatilsynet acts a a supervising body for norwegian and maintains the compliance of the privacy regulations through various routes such as dialogue, complaints handling and inspections and information.The use of data breach notifications are also a necessity in section 16 of the act.The age of consent listed under the GDPR is different then what's listed under section 5 of the act. The age of consent in relation to information society services is 13 years old. When children reach the age of 13 they may consent to the sharing and processing of their own personal data in certain situations. If their data falls within article 9 or 10 of the GDPR then the age of consent moves up to 18(*Norway - Data Protection Overview* 2024). The use of video surveillance according to section 9-5 of the working environment act and regulation on camera surveillance in the workplace, video surveillance of employees must only be performed when such a measure is objectively justified and does not involve the undue strain on employees.Video surveillance of office must only be used to help prevent hazardous situations and help safeguard the safety of the employees(*Norway - Data Protection Overview* 2024). Employer access to employee emails and other electronically stored materials is permitted if it is either necessary to safeguard the company's business or other legitimate interests(*Norway - Data Protection Overview* 2024). It is also permitted if it is believed that the employee's use of email is a breach of the employee's obligations causing possible harm to the organization. The email monitoring regulation provides several requirements in relation to the above including a duty to notify the employee and the employees right to be present during a review(*Norway - Data Protection Overview* 2024). The

Act as of July 1, 2022 covers the processing of data in credit information activities. This act sets out specific tiles for the processing of data as part of the credit information activities(*Norway - Data Protection Overview* 2024). This act replaces the former licensing requirements meaning that all former licenses from datatilsynet are now repealed.

Data Protection Act 2018/GDPR for France

Data protection in France is governed by the French Data Protection Act, or Loi Informatique et Libertés in French, and is in alignment with the European Union GDPR. The Act is overseen by the Commission Nationale de l'Informatique et des Libertés (CNIL) who are responsible for enforcing the DPA.This includes informing French citizens of their data privacy rights, the protection of data privacy rights, and the regulation and advising of the French government. This Act applies to natural or legal French citizens who process whole or partial personal data using automated or manual methods. This Act also applies to organizations located in France, government bodies, and any other public establishment that offers services of processing personal data of French citizens. The Act also applies to data controllers, data processors, subcontractors with proper third-party risk management, and other entities that process, store, transfer, or collect personal data of French citizens ("French Data Protection Act: An Overview of Data Privacy in France," n.d.). Operating with personal data under the DPA includes the following: collecting, recording, organization, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction (Saarinen, Auvray, & Cruchet, n.d.). For organizations who process data through human resource management, information technology, or clients and prospects, the following also apply when operating with personal data:

recruitment, payroll, client and prospective client files, whistleblowing hotlines, CCTV, and electronic devices (Saarinen, Auvray, & Cruchet, n.d.). The DPA must align with the EU GDPR. In the instance that there is a conflict in rules, the GDPR takes precedence (Saarinen, Auvray, & Cruchet, n.d.). The rules of the DPA apply to data subjects living in France even if the data controller is not based in France. Processing certain data requires authorization, however the initial requirements with the CNIL are removed under the GDPR. The exemptions to this include the following processes of personal data: Processing health data, processing on behalf of the state, and processing security numbers (Saarinen, Auvray, & Cruchet, n.d.). Health data processing must be "compatible with the CNIL's certification criteria or standard regulations; and implemented after the data data controller has submitted a declaration of certified conformity" (Saarinen, Auvray, & Cruchet, n.d.). When processing on behalf of the state in relation to national security, defense, public health, or law enforcement, a relevant minister must authorize it after a notice from the CNIL (Saarinen, Auvray, & Cruchet, n.d.).

Obligations of the Data Protection Act of 2018

1. **Lawfulness, Fairness and Transparency**
    a. Personal data must be lawfully processed and in a transparent manner in relation to the data being transferred. *(Quick Guide to the Principles of Data Protection)*
2. **Purpose Limitation**
    a. Personal data must be collected for a specified and legitimate purpose, which is determined at the time of collection, and must not be further processed after the purpose is finished. *(Quick Guide to the Principles of Data Protection)*
3. **Data Minimisation**

   a. All controllers only collect and process personal data that are relevant and limited to the purpose of the data collection. *(Quick Guide to the Principles of Data Protection)*

4. **Accuracy**
   a. All data collected must be up to date and accurate according to the data holder. *(Quick Guide to the Principles of Data Protection)*

5. **Storage Limitation**
   a. Controllers must hold all personal data for no longer than necessary for its intended purpose. *(Quick Guide to the Principles of Data Protection)*

6. **Integrity and Confidentiality**
   a. All data must be processed by controllers in a manner that ensures the appropriate level of security and confidentiality. *(Quick Guide to the Principles of Data Protection)*

7. **Accountability**
   a. All collectors of data must be compliant and responsible for the principles of data collection. *(Quick Guide to the Principles of Data Protection)*

Insurance and Payment

Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS outlines the cardholder data and sensitive authentication data which together make the account data that the PCI DSS requirements apply to. This account data includes:

Account Data

Cardholder Data	Sensitive Authentication Data
● Primary Account Number (PAN) ● Cardholder Name ● Expiration Date ● Service Code	● Full Track Data (magnetic-stripe data or equivalent on a chip) ● Card Verification Code ● PINs/PIN blocks

These two subsections of data must be treated differently based on the requirements. For instance, the cardholder data can be stored but "Storage is kept to a minimum". (*Payment Card Industry Data Security Standard Requirements and Testing Procedures* 2022) The PAN must be stored in an unreadable fashion, while the rest of the cardholder data can be readable in storage. However, this is completely different for the Sensitive Authentication Data which "Cannot be stored after authorization" (*Payment Card Industry Data Security Standard Requirements and Testing Procedures* 2022) and "data stored until authorization is complete must be protected with strong cryptography" (*Payment Card Industry Data Security Standard Requirements and Testing Procedures* 2022).

While the PCI DSS requirements also outline, “Entities that outsource their payment environments or payment operations to third parties remain responsible for ensuring that the account data is protected by the third party per applicable PCI DSS requirements.” (*Payment Card Industry Data Security Standard Requirements and Testing Procedures* 2022) So the third-party PCI service provider chosen should be assured to follow the PCI DSS requirements as the school can be liable for their misuse of the data from these sites. Since the third-party service provider will require access to the data the PCI traffic should be securely tunneled between the Oracle database in the cloud infrastructure and the third-party service provider site.

The PCI DSS requirements identify its scope to include, “The cardholder data environment (CDE), which is comprised of: – System components, people, and processes that store, process, and transmit cardholder data and/or sensitive authentication data, and, – System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD. AND System components, people, and processes that could impact the security of the CDE.” (*Payment Card Industry Data Security Standard Requirements and Testing Procedures* 2022) The workstations that the staff will use to input the patients', students', or employees' PCI information will need to be physically connected workstations. For this reason, all workstations that are used by the staff that would be used to take and manage the PCI information will be within the scope of these requirements. This would also indicate that any device connected to a computer VLAN (a VLAN with a purpose of 1) will fall under the scope of the requirements since they will have unrestricted access to the other workstations connected to their floor.

The principle PCI DSS requirements outline the basic measures that other than properly managing the account data as outlined above include: “Build and Maintain a Secure Network and Systems … Maintain a Vulnerability Management Program … Implement Strong Access Control Measures … Regularly Monitor and Test Networks … Maintain an Information Security Policy” (*Payment Card Industry Data Security Standard Requirements and Testing Procedures* 2022) These requirements outline that the PCI DSS standards require the full network to be secure as access to any device on the network, or any user account that is not securely configured could lead to unauthorized users gaining access to the PCI data. So these measures need to be taken in stride to provide the proper security required for such sensitive information.

The Azure cloud infrastructure which holds the Oracle database will be used to store the cardholder information so it falls under the scope of the PCI DSS requirements. The PCI data being sent between sites and the cloud needs to be securely tunneled using the certificate-based encryption put in place to make sure both end keys are authenticated as well as keep the data confidential. The account data needs to remain encrypted when at rest, and the sensitive authentication data needs to be removed from storage once it is shared with the PCI service provider.

A specific PCI DSS officer must be employed per site to process the PCI records for each site. The PCI DSS officer will also be responsible and accountable for PCI DSS compliance for this assigned site. While also being in charge of assessing the PCI DSS compliance of the third-party PCI service provider.

HIPAA

The medical school will be bound to the regulations of HIPAA since, “Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity” (*Summary of the HIPAA privacy rule* 2022)

In accordance to HIPAA Guidelines, we will adhere to the following:

We will adhere to the Privacy Rule, which is set to protect national standards to protect individual medical records and other individual private and sensitive information, which is collectively referred to as “protected health information”. This rule also gives individuals rights over their protected health information without any risks of their integrity, confidentiality and availability, such as rights to examine and obtain a copy of their health records. (*Summary of the HIPAA privacy rule* 2022)

The Privacy Rule contains exceptions, which includes:

- Victims of domestic violence and assault.
- Judicial and administrative proceedings.
- Cadaveric organ, eye and tissue donation.
- Workers compensation.

We will adhere to the Security Rule, which establishes the national standards to protect an individual's electronic personal health information that is created, received and protected by a

private entity. We are required to appropriate administrative, physical and technological safeguards to ensure the CIA Triad is not violated. (*Summary of the HIPAA privacy rule* 2022)

Upon a Breach, we will be required to notify the affected patients, HHS and the Media in some cases. A breach is defined as an unpermitted use or disclosure under the Privacy Rule that compromises security and integrity of the company that holds the information. (*Summary of the HIPAA privacy rule* 2022)

The international disease codes (the current version being ICD-10) are used to identify specific diseases and injuries both for statistical purposes and for medical billing. These codes will need to be shared from the sites to the cloud infrastructure to be stored and then forwarded to the insurance service providers when payment is due. This information would fall under the classification as Protected Health Information (PHI) so it will be bound to the regulations of HIPAA.

GDPR

The medical school, to be more specific, the campus located in the EU region, will also be bound to the regulations of GDPR (General Data Protection Regulation). All data gathered and how their usage will be informed to individuals to remain individuals rights. Individuals can access and correct the data about themselves, if needed, our organization can help in transferring their data to other organizations. In accordance with Art. 5 of GDPR (2016), we will put strictly protection and process to all health data collected, and make sure that while handling these personal data, we will maintain these key principles:

- Processing “lawfully, fairly and in a transparent manner”

- Gather data for “specified, explicit and legitimate purpose” and should be limited to what is necessary.

- Maintaining personal information’s integrity and confidentiality in a timely manner.

- Regularly use and test security measures protecting the data and process.

Upon breaching, individuals that suffer a personal data breach will get a notification not later than 72 hours after having become aware of it, which is shown at Art. 33 of the regulation. This notification will describe the case and address appropriate countermeasures to mitigate potential adverse effects.

Article 17 of GDPR regulation mentioned that personal information could be erased upon request. The medical school also follows this right to be “forgotten”, allows users to request to erase their data in the database through a considerable process, including:

- Receive requests from individuals, which could be either verbally or in hand-written. Individuals should provide specific information including their confirmation of identity, what data they want to erase and reason for the erasure.

- Respond requests, whether erase the data they want to or respond with a valid reason why the data cannot be erased.

Reasons for data cannot be erased was listed Article 17 of GDPR, for example:

- The data is being used to comply with a legal obligation.
- The data is in use for public interest purposes.
- The data is used for scientific or research purposes.
- The data is part of a legal defense.

CCPA

The medical school also follows the California Consumer Privacy Act (CCPA) which gives consumers control over the personal information that we are collecting, especially for those who are related to California residents. Our organization will ensure the protection of personal information and upholding data rights granted to California residents, including confirmed to customers what personal information we gathered and what we do with that data, as other rights as lists in CCPA as “delete your personal information, … not to sell or share your personal information, to correct inaccurate information … about you, and to limit businesses’ use and disclosure of your sensitive personal information”.

Upon breaching, individuals that suffer a personal data breach will get a notification no later than 30 days after having become aware of it, which is shown at Section A.8 of the regulation. This notification will describe the case and address appropriate countermeasures to mitigate potential adverse effects.

Regarding to request to delete personal information for California residents as shown in Section D of CCPA regulations, allows California customers to request to delete their personal data in the database through a considerable process, including:

- Receive requests from individuals, which could be either verbally or hand-written forms, or by email. Individuals should provide specific information including their confirmation of identity, what data they want to erase and reason for the erasure.

- Respond requests, whether erase the data they want to or respond with a valid reason why the data cannot be erased. Respond to the request must within 45 calendar days, which can be extended another 45 calendar days (90 days total) after notify the request illustrating in Section D.3 of the regulations.

Reasons for data cannot be delete was listed Section D.5 of CCPA, for example:

- The request cannot be verified.

- The data is publicly available information such as your address, etc.

- If the request or the deletion may potentially affect security measures.

- The data is part of a legal defense.

- "If the personal information is certain medical information, consumer credit reporting information…"

For more information, check California Legislative Information. (2018) Civil Code sections 1798.105(d) and 1798.145 for more exceptions.

VCDPA

This hospital is in compliance with any and all records of the Virginia consumer privacy act (VCDPA).The VCDPA gives consumers the right to delete and empowers the residents of virginia to request the deletion of personal data.The VCDPA also allows for consumers to request that the controller of their personal data complies with the following(*Virginia Consumer Data Protection Act* 2023). One, confirms if the controller is actually processing their personal data(*Virginia Consumer Data Protection Act* 2023). Two, Corrects inaccuracies in the consumers personal data that is collected by the controller(*Virginia Consumer Data Protection Act* 2023). Three, Deletes personal data provided by or obtained about the consumer(*Virginia Consumer Data Protection Act* 2023). Four, obtains copies of the personal data collected by the controller. Six, opts out of the processing of personal data for the purposes of targeted advertising, the sale of personal data or further profiling(*Virginia Consumer Data Protection Act* 2023). According to the VCPA consumers also have the right to submit requests to businesses to retrieve the data that is being held. This only applies to businesses that target virginia consumers for products or services that also fall under one of the follow:

- Control or process personal data of at least 100,00 consumers
- Control or process personal data of at least 25,000 consumers and drive over

Consumers are not allowed to submit requests relating to data under the VCDPA to state and local governments, any non profit organization, education or anything else listed under Va. Code

59.1- 576(B)(*Virginia Consumer Data Protection Act* 2023). Sensitive data is also considered as personal data under the VCDPA but is subject to additional requirements. The VCDPA considers the following to be sensitive data(*Virginia Consumer Data Protection Act* 2023):

- A person's race, ethnicity, religion, sexual orientation or citizenship
- The personal data collected from a child (Under the age of 13)
- Precise geolocation data
- The processing of genetic data for the purpose of uniquely identifying that person

For any questions regarding the VCDPA or how we stay in compliance please call the VCDPA Consumer protection hotline at 1-800-552-9963 if you are calling from Virginia. If not please call (804) 786-2042. The business hours are from 8:30 a.m. to 5:00 p.m, Monday through Friday.

Appendix

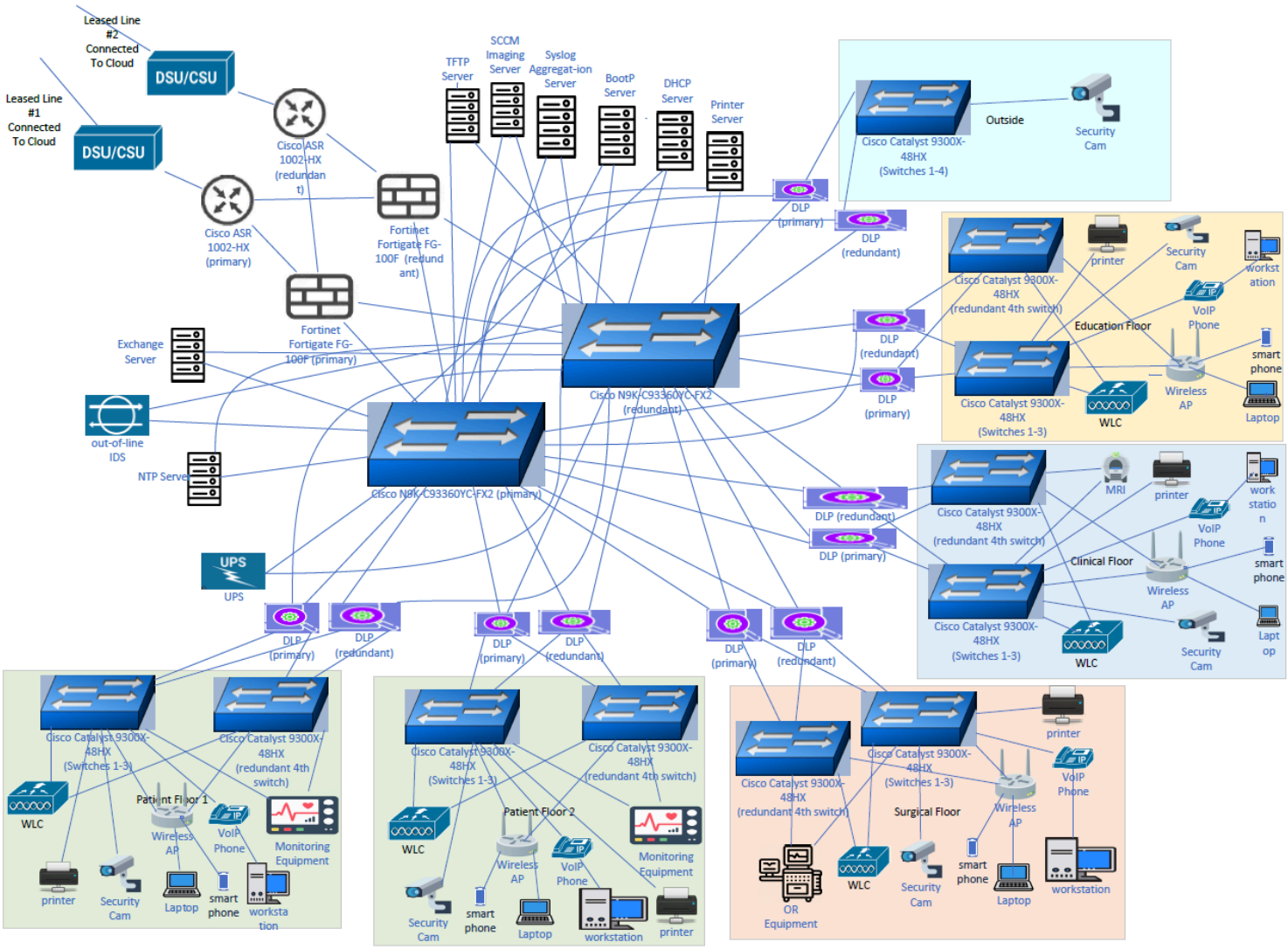

Figure 1: Generic Campus Site Network Diagram

Figure 1 represents the LAN infrastructure that each of the campus sites would be built from. Though the connections represented do not show the exact amount of devices to improve its readability. For instance there would be 32 security cameras connected to the outside switch, but only 1 is represented. The network service servers represented would be virtualized on the VMware servers. But they are shown individually in the diagram to represent where each of

these services would be configured. The redundancy for the network service servers is not represented here since they would be virtualized on multiple of the VMware servers, but again it limits the amount of objects on the diagram for readability. But for all of the network and security devices the redundancy is either shown with objects or written in the description such as with the IDF switches.

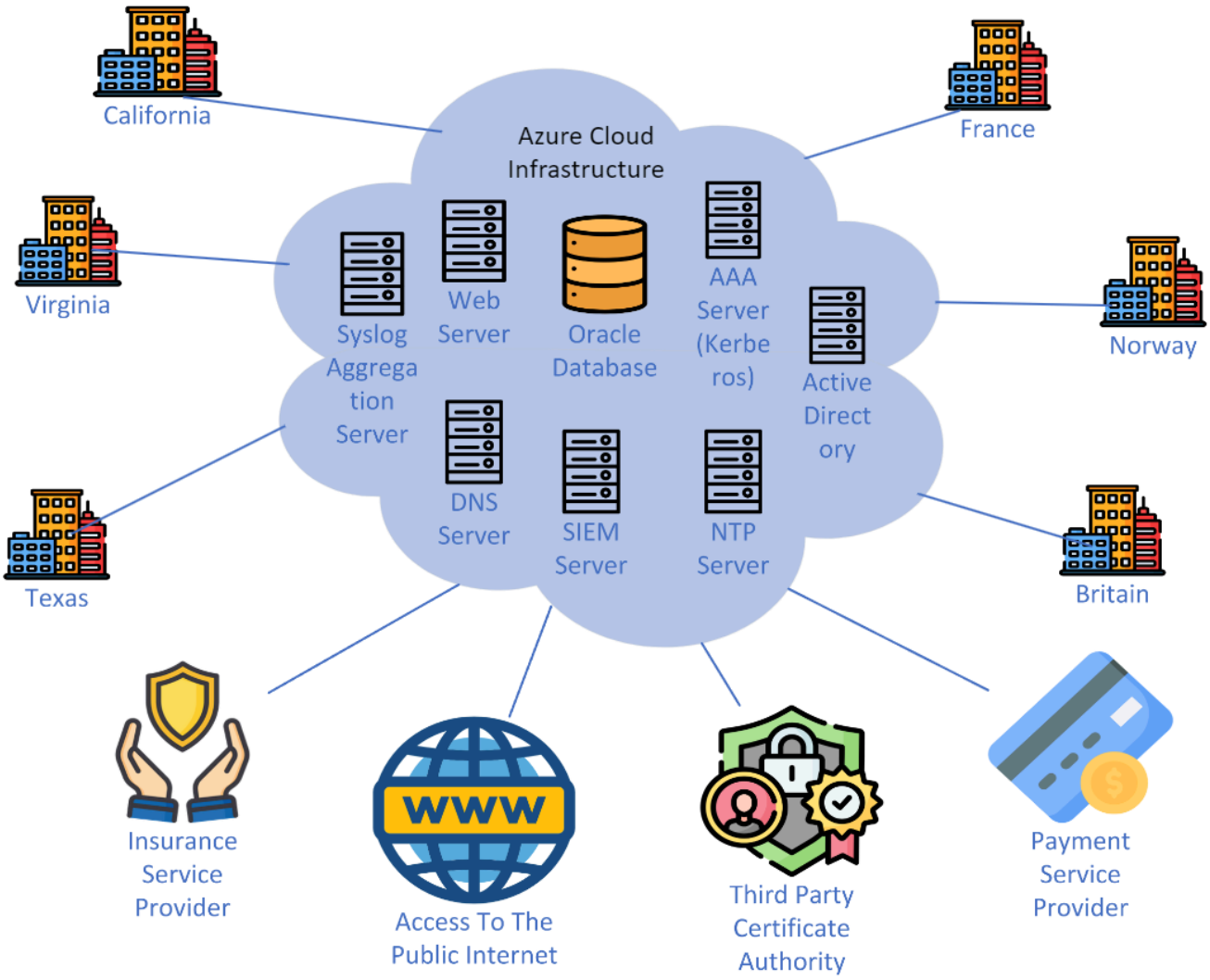

Figure 2: Azure Cloud Infrastructure Connection To Sites, Third Party Service Providers, and Public Internet

Figure 2 represents the Azure Cloud Infrastructure that each of the sites. The connection between each of the sites (labeled with their location) contains two dedicated leased line connections which lead directly from the site to the Azure Cloud Infrastructure. The connection between the insurance service provider, the third party certificate authority and the payment service provider

will be provided through a connection to the public internet. The network service servers shown inside the azure cloud infrastructure would not be individual physical servers, but virtualized on the Azure managed cloud enterprise architecture.

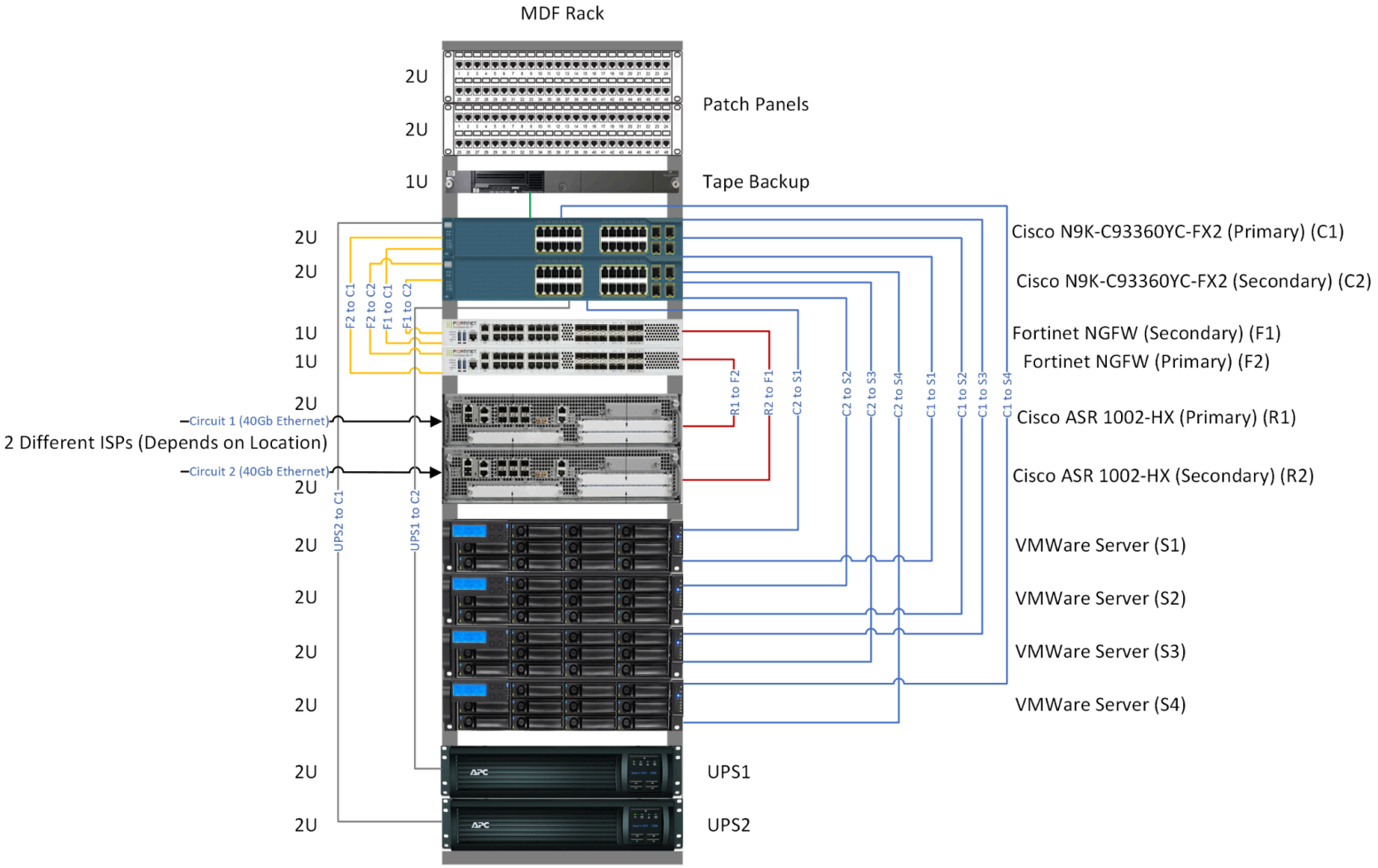

Figure 3: MDF Diagram for racks at Hospital/Campus sites

Figure 3 represents the MDF layout and includes the connections between the leased lines and routers, routers and NGFWs, NGFWs and switches, switches and VM servers and switches and UPSs. The connections to and from the patch panels, to the IDFs and to endpoints such as the APs, medical devices, VoIP phones and any other devices were omitted to improve readability.

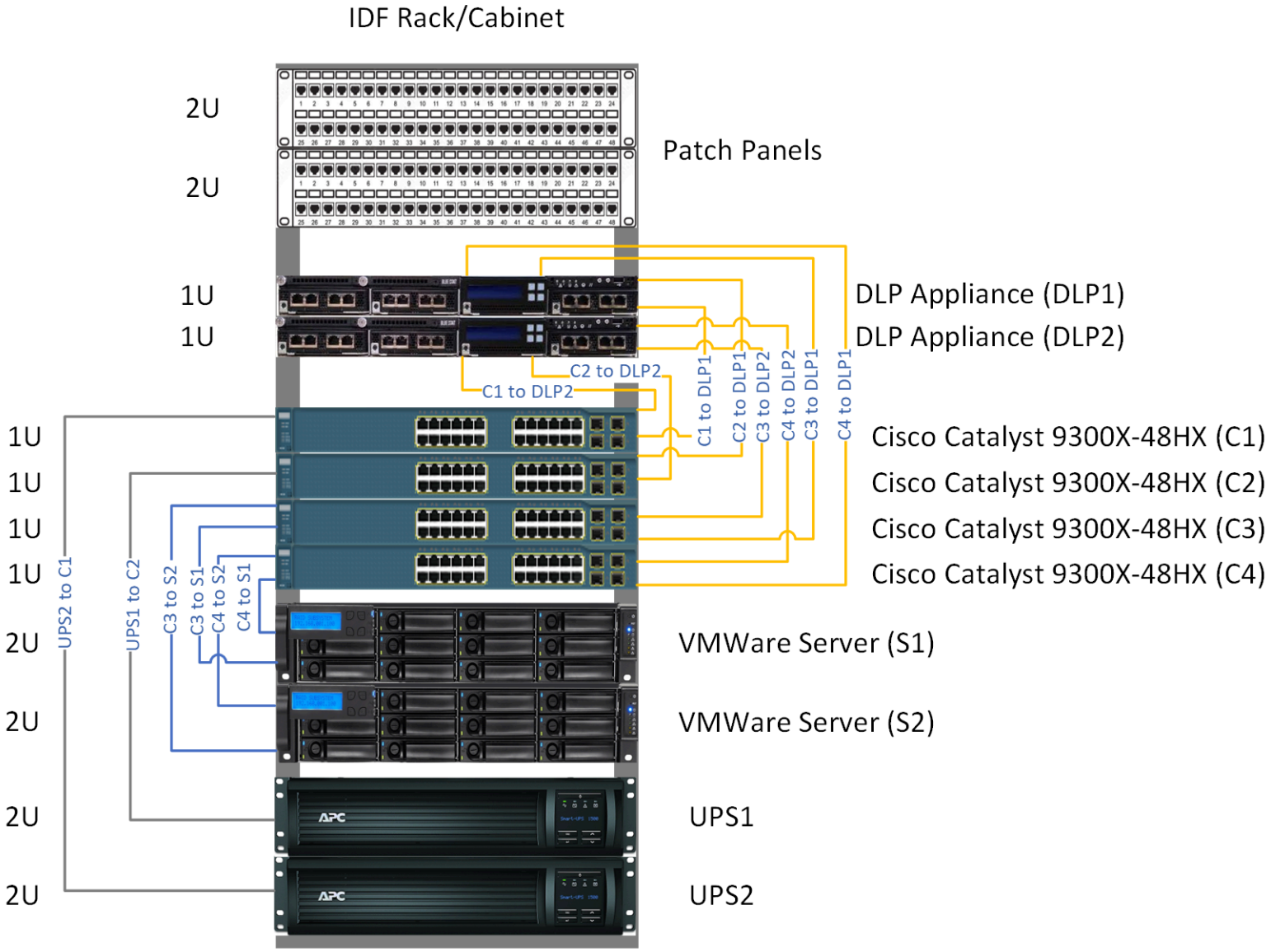

Figure 4: IDF Diagram for racks at Hospital/Campus sites

Figure 4 represents the IDF layout and includes the connections between the switches and DLP devices, switches and VM servers and switches and UPSs. The connections to and from the patch panels, to the MDF and to endpoints such as the APs, medical devices, VoIP phones and any other devices were omitted to improve readability.

References

Andress, J. (2011). Chapter 3 - Authorization and Access Control. In *The Basics of Information Security* (pp. 33–49). essay. Retrieved from https://www.sciencedirect.com/book/9781597496537/the-basics-of-information-security.

Berk-Tek. (2010, September). *Designing a reliable cabling infrastructure for healthcare facilities*. accu-tech. https://www.accu-tech.com/hs-fs/hub/54495/file-17678332-pdf/docs/nc_healthcare_white_paper_final_010511.pdf

BOOTP, DHCP, and Network Computers: Your Absolute Best Practices. MC Press Online. (1999, July 1). BOOTP, DHCP, and Network Computers: Your Absolute Best Practices - MC Press Online

California Legislative Information. (2018). Law section Title 1.81.5. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.105.&nodeTreePath=8.4.52&lawCode=CIV

CCTV camera resolution: CCTV Resolution Chart for cameras. Optiview. (2022, December 1). https://optiviewusa.com/cctv-video-resolutions/

Cisco Catalyst 9136 Series Access Points Data Sheet. Cisco. (2024, February 26). https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/nb-06-cat9136-access-point-ds-cte-en.html

Cloudflare. (n.d.). What is the right to be forgotten? https://www.cloudflare.com/learning/privacy/right-to-be-forgotten/

Data Protection Act 2018. Legislation.gov.uk. (2018, May 23). https://www.legislation.gov.uk/ukpga/2018/12/enacted#:~:text=An%20Act%20to%20make%20provision,practice%3B%20and%20for%20connected%20purposes.

Ellucian Cloud Software Standards. (n.d.). https://www.ellucian.com/assets/en//cloud-standards-june-2020-january30-2022.pdf

ErikjeMS. (2024, April 30). *Network requirements for Windows 365*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-365/enterprise/requirements-network?tabs=enterprise%2Cent

Frankel, J., Wilén, J., & Hansson Mild, K. (2018). Assessing exposures to magnetic resonance imaging's complex mixture of magnetic fields for in vivo, in vitro, and epidemiologic studies of Health Effects for staff and patients. *Frontiers in Public Health*, *6*. https://doi.org/10.3389/fpubh.2018.00066

French Data Protection Act: An Overview of Data Privacy in France. Kiteworks. (n.d.). https://www.kiteworks.com/risk-compliance-glossary/french-data-protection-act/

GDPR. (2022, September 27). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Knapp, E. D., & Langill, J. T. (2015). Chapter 12 - Security Monitoring of Industrial Control Systems. In *Industrial Network Security Securing Critical Infrastructure Networks for Smart*

Grid, SCADA, and Other Industrial Control Systems (2nd ed., pp. 351–386). essay, Elsevier Inc. https://www.sciencedirect.com/science/article/abs/pii/B9780124201149000125

Leaders, O. T. (2023, April 26). *What is a HIPAA-compliant infrastructure?*. Healthcare IT News. https://hitconsultant.net/2023/04/26/hipaa-compliant-infrastructure/

Microsoft. (2024, January 21). *Health Insurance Portability and accountability act (HIPAA) & health information technology for economic and clinical health (HITECH) act - microsoft compliance*. Microsoft Compliance | Microsoft Learn. https://learn.microsoft.com/en-us/compliance/regulatory/offering-hipaa-hitech

Norway - Data Protection Overview. DataGuidance. (2024, April 17). https://www.dataguidance.com/notes/norway-data-protection-overview

OGA. (2024, March 13). California Consumer Privacy Act (CCPA). Office of Governmental Affairs. https://www.oag.ca.gov/privacy/ccpa

Painter-Wakefield, C. (2024, August 26). *A Practical Introduction to Databases*. 3.3. Normalization. https://runestone.academy/ns/books/published/practical_db/PART3_RELATIONAL_DATABASE_THEORY/03-normalization/normalization.html

Payment Card Industry Data Security Standard Requirements and Testing Procedures. PCI Security Standards Council. (2022, March 15). https://www.pcisecuritystandards.org/document_library/

Philpott, D. R., & Gantz, S. D. (2013). Chapter 2: FISMA and the Risk Management Framework. In *FISMA and the Risk Management Framework* (pp. 23–52). essay. Retrieved from https://www.sciencedirect.com/book/9781597496414/fisma-and-the-risk-management-framework#book-description.

Quick Guide to the Principles of Data Protection. (n.d.). https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf

Saarinen, M., Auvray, E., & Cruchet, F. (n.d.). *Data Protection in France: Overview*. Latham & Watkins LLP. https://www.lw.com/en/insights/2019/01/data-protection-in-france-overview

Speed guide. epic. (n.d.). https://www.epic.com.mt/speedguide/

Summary of the HIPAA privacy rule. HHS.gov. (2022, October 19). https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=The%20Privacy%20Rule%20protects%20all,electronic%2C%20paper%2C%20or%20oral.

Surveillance storage calculator: Seagate US. Seagate.com. (n.d.). https://www.seagate.com/video-storage-calculator/#

Time Sync for windows VMS in Azure - Azure Virtual Machines. Azure Virtual Machines | Microsoft Learn. (2022, October 12). https://learn.microsoft.com/en-us/azure/virtual-machines/windows/time-sync

Virginia Consumer Data Protection Act. (n.d.).

https://www.oag.state.va.us/consumer-protection/files/tips-and-info/Virginia-Consumer-Data-Protection-Act-Summary-2-2-23.pdf