**Submitted by: Avneet Singh**

**(200468080)**

**How can we transfer personal data securely within their network?**

There are various ways to transfer personal data securely within the network of hospital. Some of the examples are given below:

1) Email Encryption - Many vendors today offer a range of products that can encrypt emails and ensure secure transfer of data. The receiver can also use the same encryption method from their end. This method is mostly web-based and works by sending the recipient a link, who then logs into a secure email-server after clicking it. From there the recipient can safely view the email message along with any attachments. The email server is either outsourced to a vendor or owned by the organization itself.

2) SHTP - Secure Hyptertext Transfer Protocol is typically used to transmit hyper text files between a server and browser. The default settings of HTTP don’t allow it to carry out any data encryption or user authentication. To keep information transmission secure, you need to add encryption to HTTP, which is done by using Transport Layer Security or TLS. Secure HTTP or HTTPS as you may call it, is supported by most of the web servers. HTTPS provides server end authentication and allows the server to validate the client or use any authentication service.

3) Website Encryption - This method of securing data is for businesses that collect sensitive customer data from their website. In our case, where we have the data of patients of a local hospital, this could be particularly useful. The general practice to secure data entered in a website is to use a Secure Sockets Layer (SSL) for encryption, which allows secure transfer of data over the website. Though it is not possible to totally eliminate the security risks, you can greatly minimize the risk of data breach.

**What Privacy Policies should we be aware of before we get started? Can you give us a checklist to follow?**

The below checklist of Privacy policies should be followed before getting started:

* **Policy and governance**. Develop a comprehensive data governance plan that outlines organizational policies and standards regarding data security and individual privacy protection.The plan should clearly identify staff responsibilities for maintaining data security and empower employees by providing tools they can use to minimize the risks of unauthorized access to PII. Refer to PTAC’s Data Governance Checklist for more information.
* **Physical security**. Make computing resources physically unavailable to unauthorized users. This includes securing access to any areas where sensitive data (i.e, data that carry the risk for harm from an unauthorized or inadvertent disclosure) are stored and processed, such as buildings and server rooms. An unlocked server room is an invitation for malicious or accidental damage. Monitor access to these areas to prevent intrusion attempts (e.g., by administering identification badges and requiring staff and visitors to log in prior to entering the premises or accessing the resources).
* **Network mapping**. Network mapping provides critical understanding of the enterprise (servers, routers, etc.) and its connections. Furthermore, network mapping can capture applications and associated data. A robust mapping capability will map the dependencies between applications, data, and network layers, and highlight potential vulnerabilities. There are a number of network mapping tools available.
* **Inventory of assets**. The inventory should include both authorized and unauthorized devices used in your computing environment. These devices are often scanned and discovered by automated programs (continuously searching the internet for vulnerabilities) and if unsecured devices are discovered they can be compromised. Inventorying, when used in conjunction with network mapping, will give your organization a better understanding of the security requirements needed to protect your assets.
* **Authentication**. The ways in which someone may be authenticated fall into three categories: something you know, something you have, or something you are. Two-factor authentication (TFA) combines two of these elements and is more costly, but provides more security. Consider TFA for remote users or privileged “super users.” Authentication technologies provide assurance that the person is authorized to access network assets, services, and information.
* **Provide a layered defense**. Employ a “Defense in Depth” architecture that uses a wide spectrum of tools arrayed in a complementary fashion. The most common layers to protect are hosts (individual computers), application, network, and perimeter. There are specific security controls that are suited for use at each of these layers. Relying on a firewall alone to protect your network is never adequate.
* **Secure configurations**. It is a best practice not to put any hardware or software onto your network until it has been security tested and configured to optimize its security. Continuous scanning to ensure system components remain in a secure state is a critical capability that will enhance data security protection. Proactive management of security risks also involves establishing a comprehensive change management program to analyze and address security and privacy risks introduced by new technology or business processes.
* **Access control**. Securing data access includes requiring strong passwords and multiple levels of user authentication, setting limits on the length of data access (e.g., locking access after the session timeout), limiting logical access to sensitive data and resources, and limiting administrative privileges. Role-based access is essential for protecting PII and sensitive data; defining specified roles and privileges for users is a required security procedure. Sensitive data that few personnel have access to should not be stored on the same server as other types of data used by more personnel without additional protections for the data (e.g., encryption).
* **Firewalls and Intrusion Detection/Prevention Systems (IDPS).** A firewall is a device designed to permit or deny network transmissions based upon a set of rules. Firewalls are frequently used to protect networks from unauthorized access, while permitting legitimate communications to pass. An IDPS is a monitoring device that is designed to detect malicious activity on the network. Although some automatically take remediation action, most report suspicious activity to a central monitoring point for further analysis.
* **Automated vulnerability scanning**. When new vulnerabilities (to hardware, operating systems, applications, and other network devices) are discovered, hackers immediately scan networks for these vulnerabilities. Scanning your network and systems on a regular basis will minimize the time of exposure to known vulnerabilities.
* **Emailing confidential data**. Consider the sensitivity level of the data to be sent over the email. Emailing unprotected PII or sensitive data poses a high security risk. It is recommended that organizations use alternative practices to protect transmissions of these data. These practices include mailing paper copies via secure carrier, de-sensitizing data before transmission, and applying technical solutions for transferring files electronically (e.g., encrypting data files and/or encrypting email transmissions themselves).
* **Audit and compliance monitoring**. Audits are used to provide an independent assessment of your data protection capabilities and procedures should be performed periodically. Auditors that are familiar with Family Educational Rights and Privacy Act statutory and regulatory requirements can further assist you in determining whether your systems are in compliance.

**What security policy is best for transferring personal information?**

It is important to secure the personal information from unauthorized accesses. Below policies can be best used for transferring personal information:

Cryptography allows two parties to communicate in plain sight but in a language that their adversary cannot read.To encrypt a message, the sender must manipulate the content using some systematic method, known as an algorithm. The original message, called plaintext, may be scrambled so its letters line up in an unintelligible order or each letter might be replaced with another.

The traditional file transfer protocol (FTP) is a simple way of transferring data, but it offers nothing in terms of data protection. Files are transferred without encryption, making data readable for anyone who intercepts it. While this is fine if you’re just sending unimportant files, this could lead to major data compromises if you’re sending crucial data.

SFTP, in contrast, offers a secure shell protecting files. Because files are encrypted, you don’t have to worry about data falling into the wrong hands. This is the ideal mode of transfer for any file that you want to protect. SFTP uses an encrypted type of fingerprint technology to first verify host keys before any data transfer has taken place.

**Can we encode and encrypt images?**

Yes, just like text, we can encode and encrypt the images. By running a sequence of mathematical operations, we can encrypt the images. A software key is necessary to unlock the encryption code, and it's created by the same software that scrambles the picture. The encrypted image and the key are sent to the recipient separately to minimize the chance that a hacker could intercept both.

**Our database cannot be moved from the site and we need to be able to access it externally using a secure API  
Can you explain the architecture of a secure API?**

### API Gateway : An API Gateway is a necessary component of an API security architecture because it works as a focused server that controls traffic. This capability can also detect possible attacks that will leave your APIs open and at risk.

There are many ways to secure an API security architecture, but here are a few ways to put this in place via a trusted API Gateway:

### Control :Connections to the API Gateway should be consistent and very persistent so that possible encryption cannot be recognized.

### Inaugurate sorting procedures and alarms : The API Gateway should be made to filter out requests. This should also include the ability to block out threats. Further, notification should go out when danger is imminent.

### Harness protective layers :The API Gateway should be able to provide a high-end buffering layer. This helps to protect the API from danger.

### Deploying a possible cyberattack : With an API Gateway in place, your API security architecture can indicate when an attack is about to happen. This is a win-win for all.

### Management : An API Gateway should be able to manage action for authorization. This allows for an API security architecture to have access.

### Safety : An API Gateway blocks attacks from everyone. When there is any danger to a non-secured API, this is a complete call for all API security architecture to be in place.

**Can you recommend a secure framework for coding an API?**

**I**SO 27001 and ISO 27002 : Created by the [International Organization for Standardization (ISO)](http://www.iso.org/iso/home.html), ISO 27001 and ISO 27002 certifications are considered the international standard for validating a cybersecurity program — internally and across third parties. With an ISO certification, companies can demonstrate to the board, customers, partners, and shareholders that they are doing the right things to manage cyber risk. Likewise, if a vendor is ISO 27001/2 certified it’s a good indicator that they have mature cybersecurity practices and controls in place.

**What data interchange format should we use while transferring data between locations?**

We can use

1. XML - One can put as many different types of information in the XML and it still remains simple.
2. JSON format to transfer data between locations.

JSON is a data interchange format whose design goals were to be textual, minimal, and a subset of JavaScript; it supports two structures: objects (unordered collections of name/value pairs) and arrays (ordered sequences of values), as well as four simple types: strings, numbers, booleans, and null.

**How should we store our data in our many locations?**

## **Colocation**

## Colocation is taking your server and placing it inside a data center where it shares power, network, and cooling costs with other servers. The server is still yours, you’re just renting the space.

## **Social Media Storage**

As social media profiles grew in popularity, people soon realized they served as a way to store photos and videos where they could always be accessed. This way, these digital files didn’t take up room on mobile devices or computers. Plus, these social media sites provided a way to create albums for easy access and sharing

## **Cloud Storage**

This digital storage option is increasingly popular for its many benefits, despite some shortcomings. Companies like Dropbox emerged to offer an option for digital files that addressed existing storage problems. It wasn’t long before Google Drive, Box, and numerous other cloud platforms appeared. Ref myamberlife.