Faxing: Overview

CSS utilizes fax modems in order to transmit data to clients that receive data via fax. This document is designed to provide the laboratory with guidelines to ensure their fax transmissions are HIPAA compliant. Our fax modems utilize a direct phone line connection in order to dial a fax machine on the receiving end. A standard 10-digit fax number is used to designate where the fax gets sent.

Faxing: HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules allow covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. CSS provides the following guidelines and functions in order to ensure that you are not violating HIPAA when performing transmissions via fax.

Verify Fax Machine Location: It is important to verify that the location of the fax machine to which Protected Health Information (PHI) is sent to is in a secure location that can only be accessed by approved staff.

Utilize Cover Sheets: Cover sheets are a requirement under HIPAA. CSS provides our clients with a cover sheet that contains the following: date & time sent, name of recipient, recipient's fax number, sender's name & organization, sender's phone number, and a HIPAA fax disclaimer.

Monitoring Software: CSS provides software that allows monitoring or auditing of all fax transmissions.

Faxing: Conclusion

Make sure security safeguards are in place when utilizing the fax machine to transmit PHI, and confirm your staff is properly trained on handling and transmitting patient information. Sending a fax to the wrong number is one of the most common errors, as evidenced by a number of reported breaches. Office staff should always verify the recipient's fax number and use a cover sheet to the attention of the recipient that does not include any PHI. It is the responsibility of the covered entity to ensure their fax practices comply with HIPAA Privacy Rules.

Outreach Portal: Overview

The CSS Outreach Portal provides authenticated users outside the laboratory with the ability to view their patient's results. The laboratory will appoint an individual to be the Outreach Portal Administrator.

Outreach Portal: HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules allow covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. CSS provides the following guidelines and functions in order to ensure that you are not violating HIPAA when providing patient results on the web.

Access Control: The Outreach Portal Administrator will ensure that only approved users have credentials to access the system. Proper password strength guidelines and safeguards should be followed by all users of the Outreach Portal.

Audit Controls: Software mechanisms are in place that allow auditing of the system. Auditing can be performed from within Avalon or directly through SQL.

Integrity Controls: Integrity controls are provided that allow the Outreach Portal Administrator to tailor access as needed. Electronic measures based on administrative settings are put in place to confirm that e-PHI has not been improperly altered or destroyed.

Transmission Security: An SSL certificate is utilized to ensure that e-PHI being transmitted is encrypted and guarantees the identity of the Outreach Portal.

Outreach Portal: Conclusion

The biggest vulnerability with the Outreach Portal is the user. The Outreach Portal Administrator should advise all users of the system of proper password strength and storage. All passwords are stored encrypted and can be reset by the Outreach Portal Administrator. All e-PHI viewable in the system is backed up. An SSL certificate is utilized to ensure the identity of the Outreach Portal and that all data being transmitted is encrypted.

SSH: HIPAA Compliance

In order to provide technical assistance and maintenance CSS's support team utilizes SSH to connect to your laboratories server . SSH is utilized over telnet simply because telnet doesn't encrypt data over the internet. CSS's support team ensures that all protected health information remains confidential and secure when our teams are providing support.

Regulation	CSS Solution
Workforce Security (§ 164.308(a)(3)): Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information.	Administrative controls are put in place to ensure that only authorized access is allowed onto your server.
Information Access Management (§ 164.308 (a)(4)): Implement policies and procedures for authorizing access to electronic protected health information.	Directories are segregated by level of access. Users that require access to your server will be given credentials which have access restricted according to their role in the business.
Access Control (§ 164.312(a)(1)): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.	SQL security rules and local administrative policies are in place to ensure that only Avalon and specified users are able to access protected health information.
Audit Controls (§ 164.312(b)): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Shell and SQL logging are in place to record and examine activity on the system.
Transmission Security (§ 164.312(e)(1)): Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications	SSH is utilized in tandem with strict firewall rules to encrypt traffic between both endpoints, and prevent unauthorized viewing of data from rogue devices.