New York Institute of Technology

Fall 2021

Title: Extensive Security Report for Medical Software

Yash Arun Patade

Project Contents.

Overview.

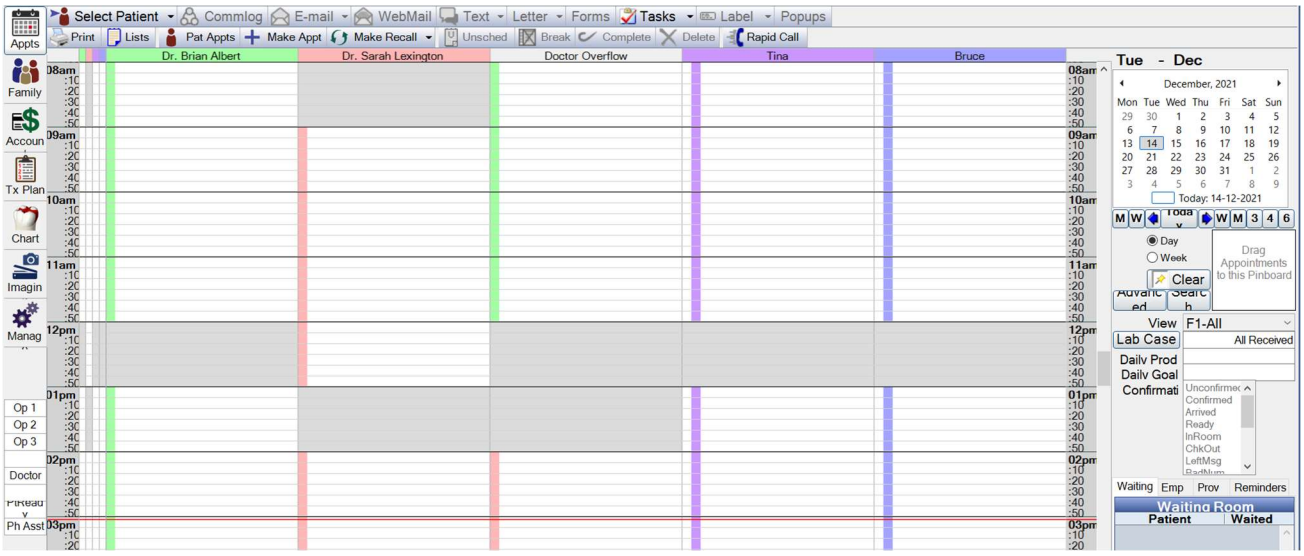
This project will implement the use of ‘Open Dental Software’ as the test subject for the risk assessment, compliance checks and creating security, business continuity, contingency, and disaster recovery plans. Also, related policies will be emphasized in this project. For the risk assessment, the SRA Risk Assessment toolkit will be used. It will assist in conducting the security risk assessment. A total of 156 questions are to be addressed to do the same. For the HIPAA compliance check, the HSR Toolkit (HIPAA Security Rule Toolkit) will be leveraged; 492 questions addressed.

Keywords: PHI – Protected Health Information, ePHI – electronic Protected Health Information, HIPAA – Health Insurance Portability and Accountability Act of 1996.

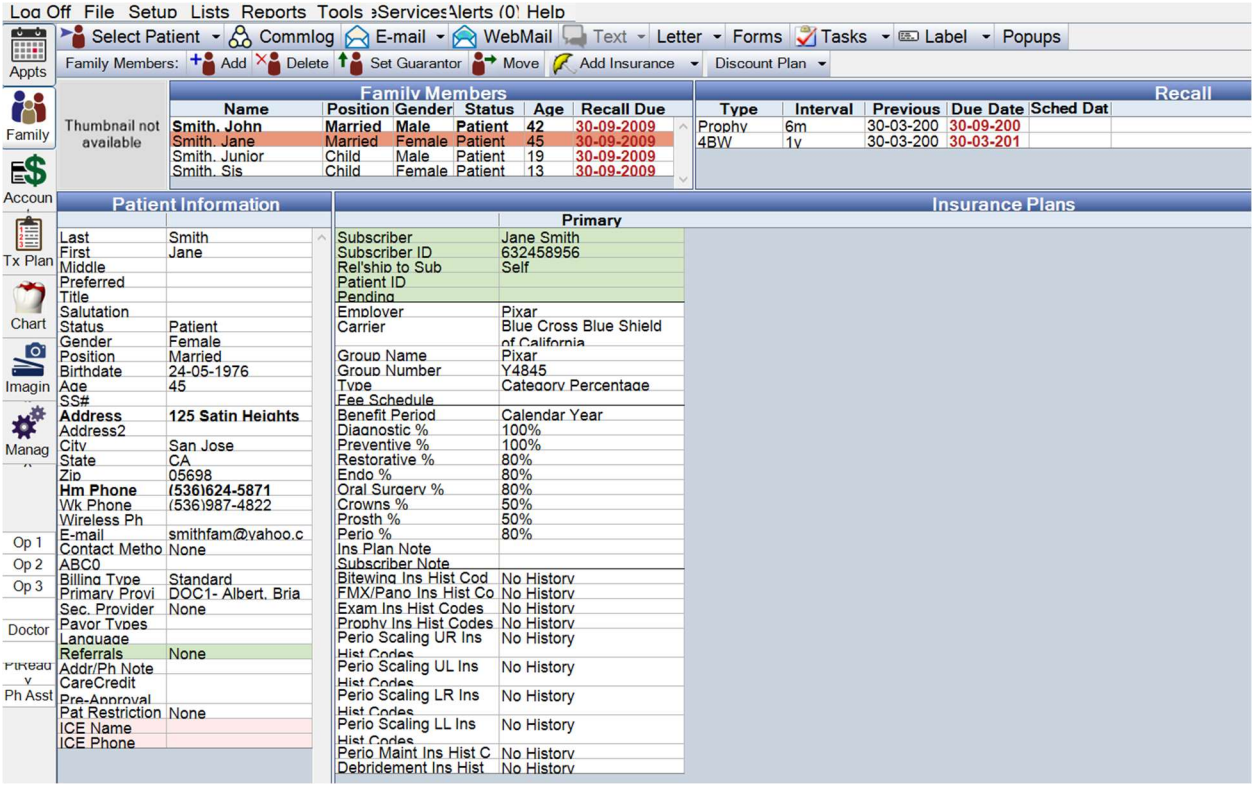
Intro to the system.

Open Dental is an open-source dental management software. For network security, a few things need to be addressed namely, the Windows firewall, MySQL Server and sharing the Open-Dental A-to-Z Folders (downloaded while installing the software). Open Dental is an open-source dental management software. The main features of the software are as follows:

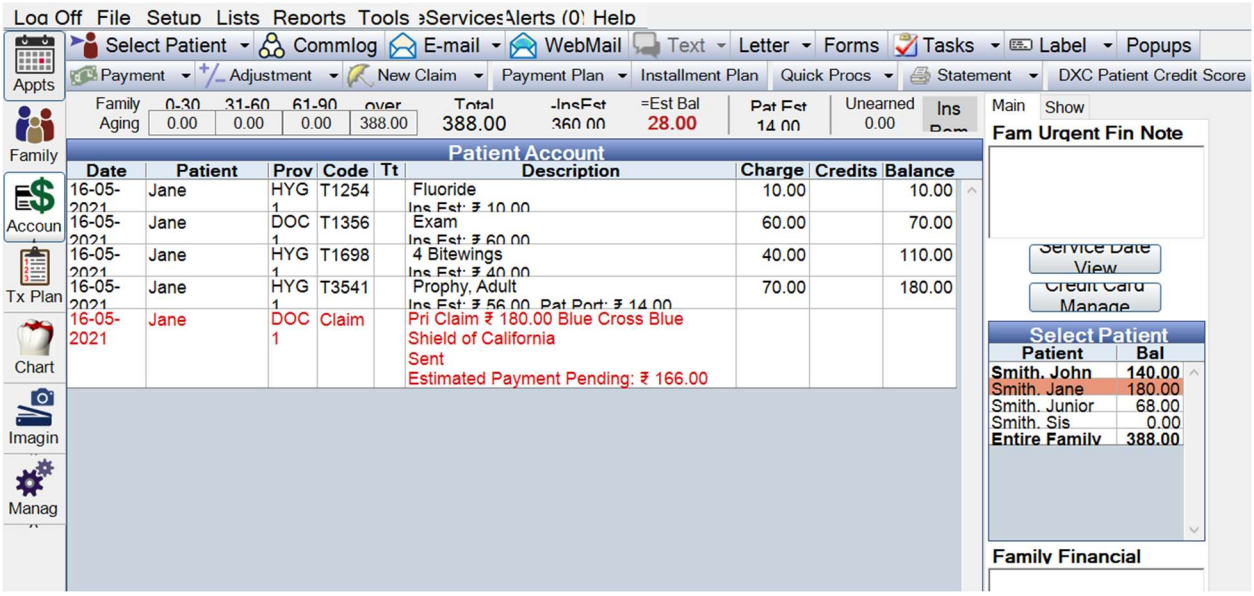
- Appointment management.



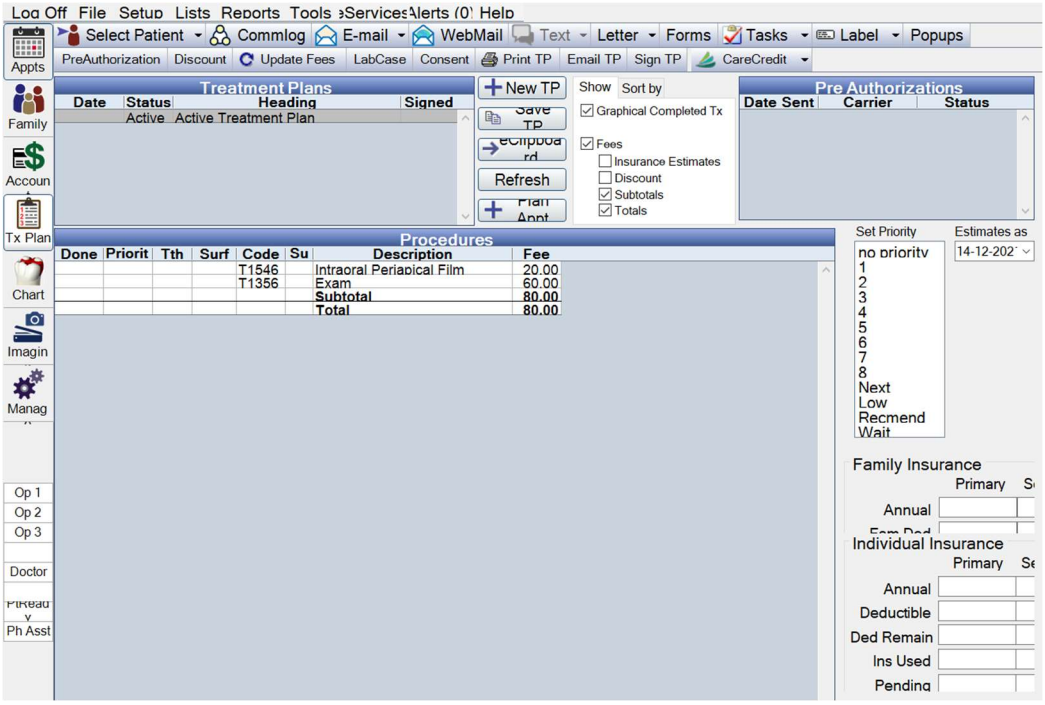
- Patient family information.



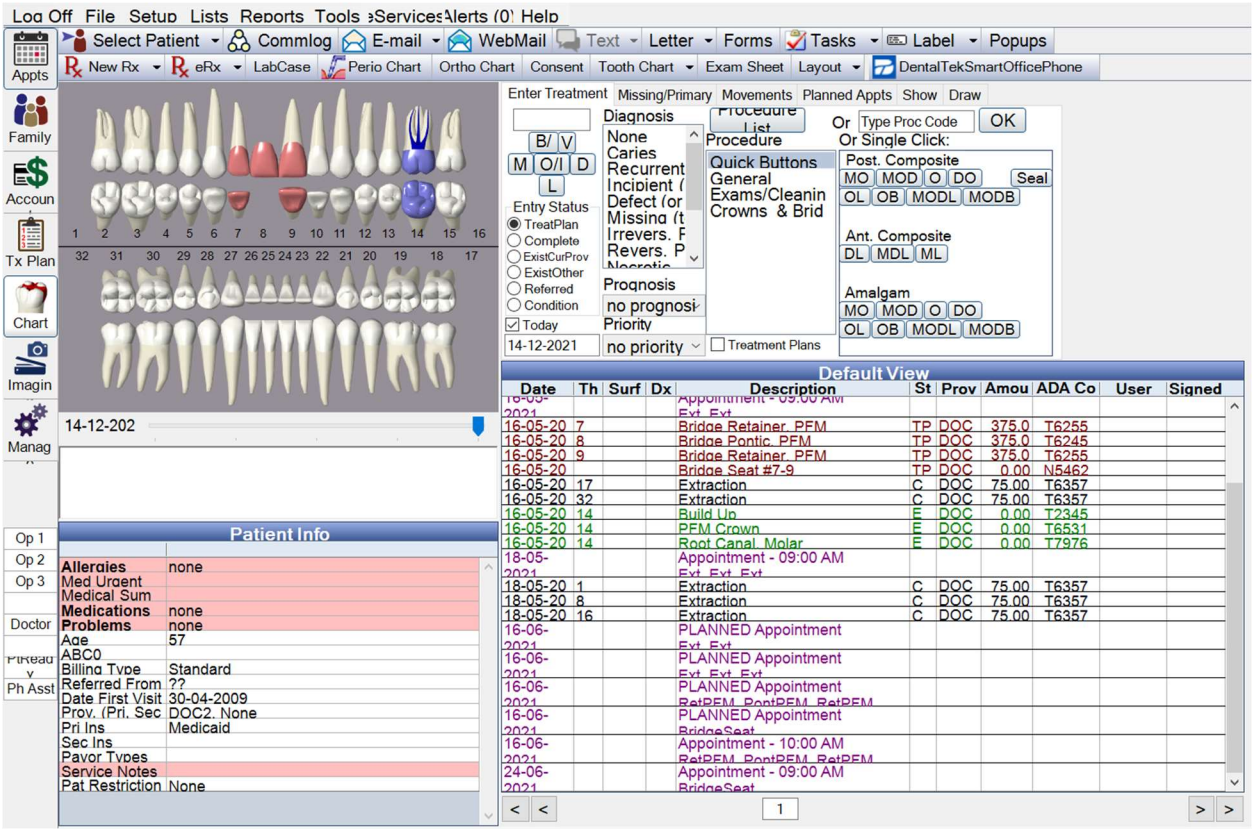
- Accounting.



- Treatment planning.



- Charting.



Strategic Plan for Information Security.

An information security strategic plan provides a sense of direction within an organization. This plan is a great tool which can be used as a guide for performing daily tasks and carry out regular decisions. The strategic plan documentation also helps the organization or company to track and evaluate progress, also to come up with new approaches as required in the future.

The following is the Strategic Plan summary for the 'Open Dental Software'. The SRA Tool is used to develop the Strategic plan report.

Has your practice completed a security risk assessment (SRA) before?	Yes.	Continuing to complete security risk assessments will help safeguard the confidentiality, integrity, and availability of ePHI.
Do you review and update your SRA?	Yes.	This is the most effective option to protect the confidentiality, integrity, and availability of ePHI.
How often do you review and update your SRA?	Periodically and in response to operational changes and/or security incidents.	This is the most effective option to protect the confidentiality, integrity, and availability of ePHI.
Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?	Yes.	This is the most effective option to protect the confidentiality, integrity, and availability of ePHI. A comprehensive security risk assessment should include all information systems that contain, process, or transmit ePHI.
What do you include in your SRA documentation?	Our SRA documentation includes possible threats and vulnerabilities which we assign impact and likelihood ratings to. This allows us to determine severity. We develop corrective action plans as needed to mitigate identified security deficiencies according to which threats and vulnerabilities are most severe.	This is the most effective option to protect the confidentiality, integrity, and availability of ePHI.

Do you respond to the threats and vulnerabilities identified in your SRA?	Yes, we respond. We also maintain supporting documentation of our response.	This is the most effective option.Threats and vulnerabilities should be documented within your SRA and given impact and likelihood ratings to determine severity. Safeguards protecting ePHI from these threats and vulnerabilities should be evaluated for effectiveness. Corrective action plans with plan of action milestones should be developed as needed to mitigate identified security deficiencies according to which threats and vulnerabilities are most severe. Risks should be formally deemed "accepted" only when appropriate.
Do you identify specific personnel to respond to and mitigate the threats and vulnerabilities found in your SRA?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you communicate SRA results to personnel involved in responding to threats or vulnerabilities?	Yes.	This is the most effective option.
How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?	Written and verbal communication as well as coordinated corrective action planning.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.Written results of the risk assessment should be communicated to the personnel responsible for responding to identified threats and vulnerabilities. The responsible persons should be involved in the creation of corrective action plans to mitigate threats and vulnerabilities for which they are responsible.

Do you maintain documentation of policies and procedures regarding risk assessment, risk management and information security activities?	Yes, we have a process by which management develops, implements, reviews, and updates security policies and procedures.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you review and update your security documentation, including policies and procedures?	Yes, we review and update our security documentation periodically and as necessary.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you update your security program documentation, including policies and procedures?	We have a periodic review of information security policies that formally evaluates their effectiveness. Policies and procedures are updated as needed.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Is the security officer involved in all security policy and procedure updates?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How does documentation for your risk management and security procedures compare to your actual business practices?	Our risk management and security documentation completely and accurately reflects our actual business practices.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How long are information security management and risk management documents kept?	We maintain documents for at least six (6) years from the date of their creation or when they were last in effect, whichever is longer. These documents are maintained and backed up.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. The federal requirement is six (6) years retention of documentation, but your state or jurisdiction may have additional requirements.
Do you make sure that information security and risk management documentation is available to those who need it?	Yes. Documentation is made available to appropriate workforce members in physical and/or electronic formats (for example, our practice's shared drive or intranet).	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

How do you ensure that security and risk management documentation is available to those who need it?	Appropriate workforce members receive instruction on our information security documentation and where to find it as part of their periodic privacy and security training. Documentation is securely made available to workforce members in physical or electronic formats.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you manage and control personnel access to ePHI, systems, and facilities?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you manage and control personnel access to ePHI, systems, and facilities?	Detailed log of personnel and access levels based on role. Updates are reviewed by the security officer.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
What is your process for authorizing, establishing, and modifying access to ePHI?	Our security procedures designate personnel authorized to grant, review, modify, and terminate access. Access levels are reviewed and modified as needed.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How much access to ePHI is granted to users or other entities?	Minimum access necessary based on the user's formal role.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How are individual users identified when accessing ePHI ?	Unique IDs and individual passwords are created for authorized workforce members and contractors in order access ePHI.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you ensure all of your workforce members have appropriate access to ePHI?	Yes. We have written procedures to ensure workforce members' access privileges are minimum necessary (i.e. "need to know") based on their roles. These access privileges are approved by the security officer.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you make sure that your workforce's designated access to ePHI is logical, consistent, and appropriate ?	Workforce members are granted access based on the minimum amount necessary for their role. This is consistently applied across the practice and any changes must be formally approved and documented.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Do you use encryption to control access to ePHI?	Yes.	This is the most effective option. Whenever reasonable and appropriate implement a mechanism to encrypt and decrypt ePHI.
What procedures do you have in place to encrypt ePHI when deemed reasonable and appropriate?	Encryption is evaluated as part of our risk management process. We have procedures in place to encrypt data at rest (for example, USB drives or tapes) and in transit (for example, email or cloud EHR) whenever reasonable and appropriate, and find an alternative safeguard when not reasonable and appropriate.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you use alternative safeguards in place of encryption?	Yes. When encryption is not reasonable or appropriate, we implement an alternative safeguard.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
When encryption is deemed unreasonable or inappropriate to implement, do you document the use of an alternative safeguard?	Yes. We have policies and procedures to identify encryption capabilities of our devices and information systems. When encryption is not reasonable or appropriate, we implement an alternative safeguard and document it.	Having policies and procedures to identify the encryption capabilities of your devices and information systems and then documenting when encryption is not reasonable or appropriate, and that you have implemented an alternative safeguard is the best practice.
Have you evaluated implementing any of the following encryption solutions in your local environment? (Full disk encryption, file/folder encryption, encryption of thumb drives or other external media)	All of the above.	Encryption in these areas is critical to protecting ePHI in your local environment.
Have you evaluated implementing encryption solutions for any of the following cloud services? (Email service, file storage, web applications, remote system backups)	All of the above.	Encryption in these areas is critical to protecting ePHI in your cloud environments.

Have you evaluated implementing any of the following encryption solutions for data in transit? (Encryption of internet traffic by means of a VPN, web traffic over HTTP encrypted email, or secure file transfer)	All of the above.	Encryption in these areas is critical to protecting ePHI in transit.
Do you periodically review your information systems for how security settings can be implemented to safeguard ePHI?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How are you aware of the security settings for information systems which process, store, or transmit ePHI?	All systems which create, receive, maintain, or transmit ePHI (including any firewalls, databases, servers, and networked devices) have been examined to determine how security settings can be implemented to most appropriately protect ePHI.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you use security settings and mechanisms to record and examine system activity?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
What mechanisms are in place to monitor or log system activity?	Monitoring of system users, access attempts, and modifications. This includes a date/time stamp.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you monitor or track ePHI system activity?	System activity records are reviewed on a regular basis. The frequency of reviews is documented within our procedures. Results of activity reviews are also maintained, including activities which may prompt further investigation.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you have automatic logoff enabled on devices and platforms accessing ePHI?	Yes, automatic logoff is enabled on all devices and platforms to terminate access to ePHI after a set time of inactivity.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Do you ensure users accessing ePHI are who they claim to be?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you ensure users accessing ePHI are who they claim to be?	Users authenticate themselves to access ePHI using the method authorized by our practice's policy and procedure (for example, user name and password, physical token, or biometric feature).	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

How do you determine the means by which ePHI is accessed?	All systems, devices, and applications which access ePHI are identified, evaluated, approved, and inventoried. Users can only access ePHI through these approved systems, devices, and applications.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you protect ePHI from unauthorized modification or destruction?	Yes. We have developed and implemented policies and procedures to protect ePHI from improper alteration or destruction.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you confirm that ePHI has not been modified or destroyed without authorization?	We have mechanisms (e.g. integrity verification tools) to corroborate that ePHI has not been altered or destroyed in an unauthorized manner or detect if such alteration occurs.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you protect against unauthorized access to or modification of ePHI when it is being transmitted electronically?	Yes. We have implemented technical security measures and procedures to prevent unauthorized access to and detect modification of transmitted ePHI.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Have you implemented mechanisms to record activity on information systems which create or use ePHI ?	Yes. Activity on systems which create or use ePHI is recorded and examined. This is documented in our procedures, including a complete inventory of systems that record activity and how it is examined.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Do you manage access to and use of your facility or facilities [i.e. that house information systems and ePHI]?	Yes. We have written procedures in place restricting access to and use of our facilities.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
What physical protections do you have in place to manage facility security risks?	We have methods for controlling and managing physical access to our facility such as, keypads, locks, security cameras, etc. We also have an inventory of our practice's facilities that house equipment that create, maintain, receive, and transmit ePHI.Our policies and procedures outline managements' involvement in facility access control and how authorization credentials for facility access are issued and removed for our workforce members and/or visitors. Workforce members' roles and responsibilities in facility access control procedures are documented and communicated.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you restrict physical access to and use of your equipment [i.e. equipment that house ePHI]?	Yes. We have written policies and implemented procedures restricting access to equipment that house ePHI to authorized users only.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you manage workforce member, visitor, and third party access to electronic devices?	Yes. We have written procedures for classifying electronic devices, based on their capabilities, connection, and allowable activities; access to electronic devices by workforce members, visitors, and/or third parties is determined based on their classification.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Do you have physical protections in place, such as cable locks for portable laptops, screen filters for screen visible in high traffic areas, to manage electronic device security risks?	Yes. We have physical protections in place for all electronic devices and this is documented in policy and procedure.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
What physical protections do you have in place for electronic devices with access to ePHI?	We have robust procedures for electronic device access control such as, authorization for issuing new electronic device access and removing electronic device access. We also use screen filters, docking stations with locks, and/or cable locks for portable devices, privacy screens [walls or partitions], and/or secured proximity for servers and network equipment.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you keep an inventory and a location record of all of its electronic devices?	Yes. Our inventory list of all electronic devices and their functions is currently documented and updated on a periodic basis.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you have an authorized user who approves access levels within information systems and locations that use ePHI?	Yes. We have written procedures outlining who has the authorization to approve access to information systems, location, and ePHI; how access requests are submitted; and how access is granted.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you validate a person's access to facilities (including workforce members and visitors) based on their role or function?	Yes. We have procedures for validating access to our facility. Access levels are based on role or function. We also have strict requirements for validating workforce members or visitors who seek access to our critical systems and software programs.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you validate a person's access to your facility?	We maintain lists of authorized persons and have controls in place to identify persons attempting to access the practice, grant access to authorized persons, and prevent access by unauthorized persons.	These are effective means of validating facility access.

Do you have access validation requirements for personnel and visitors seeking access to your critical systems (such as IT, software developers, or network admins)?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Does this include controlling access to your software programs for testing and revisions?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you have procedures for validating a third party person's access to the facility based on their role or function?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you have hardware, software, or other mechanisms that record and examine activity on information systems with access to ePHI?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
What requirements are in place for retention of audit reports?	Our practice retains records of audit report review for a minimum of six (6) years, consistent with retention requirements for all information security documentation.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Your state or jurisdiction may have additional requirements beyond the six (6) year retention requirement.
Do you maintain records of physical changes upgrades, and modifications to your facility?	Yes. We have written procedures to document modifications to our facility. This includes documenting when physical security component repairs, modifications, or updates are needed and our workforce members' roles and responsibilities in that process. Any changes to our facility's security components go through an authorization process.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

How do you maintain awareness of the movement of electronic devices and media?	We maintain a detailed inventory of all electronic devices and media which contain ePHI, including where they are located, which workforce members are authorized to access or possess the devices, and to where they are moved.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Are electronic devices secured?	Yes. We have procedures for safeguarding all electronic devices (such as screen guards, cable locks, locking storage rooms, cameras, and other physical features).	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you back up ePHI to ensure availability when devices are moved?	Yes. Our critical data and ePHI is centrally stored (such as in a cloud or active directory server) that can be accessed from any authorized device.	This is an effective option to protect the confidentiality, integrity, and availability of ePHI. Make sure backups will be available and functional when needed through periodic testing.
How do you determine what is considered appropriate use of electronic devices and connected network devices?	We have documented policies and procedures in place outlining proper functions to be performed on electronic devices and devices (e.g. whether or not they should access ePHI), how those functions will be performed, who is authorized to use the devices, and the physical surroundings of the devices.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you have procedures for terminating or changing third-party access when the contract, business associate agreement, or other arrangement with the third party ends or is changed?	Yes	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Do you ensure access to ePHI is terminated when employment or other arrangements with the workforce member ends?	Yes. We have written procedures documenting termination or change of access to ePHI upon termination or change of employment, including recovery of access control devices (including organization-owned devices, media, and equipment), deactivation of information system access, appropriate changes in access levels and/or privileges pursuant to job description changes that necessitate more or less access to ePHI, time frames to terminate access to ePHI, and exit interviews that include a discussion of privacy and security topics regarding ePHI.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you ensure media is sanitized prior to re-use?	We have a process to completely purge data from all devices prior to re-use through device reimaging, degaussing, or other industry standard method; our method conforms to guidelines in NIST SP 800-88 and OCR Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.	This is an effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Areas for Review (4%)		
Do you ensure devices which created, maintained, received, or transmitted ePHI are effectively sanitized when they are disposed of?	No. We place unused devices out of normal work areas but these are not secured.	Unused and old equipment should be stored in a secure area if it contains/contained ePHI. ePHI on these devices should be purged using a method that conforms to guidelines in NIST SP 800-88 and OCR Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

Enterprise Information Security Policy.

As an organization which handles medical data, it may need to deal with other external businesses or groups in order to get a few things done, which cannot be performed in-house. Also, this data is useful to researchers to perform analytics and deep learning to assist and further expand the research. But, to ensure the privacy of the patients, a strong policy is required.

[1] Plan a Business Associate Agreement (BAA) with all external parties involved.

- Both the organizations should be under a Business Associate Agreement, if PHI is shared to a third-party vendor or a research team.

- The BAA contract should be signed by the business associate, before handling the PHI.

- If a security breach occurs and the PHI is exposed, the BAA contract should clearly hold one party responsible.

The information security management and risk management documents should be stored and handled in an appropriate way. A strong policy needs to be in place for the employees to guide while handling the respective documents.

[2] Maintain respective documents for at least six (6) years.

- Making arrangements to maintain documents relating to security and risks for at least six (6) years, from the date of their creation or when they were last in effect, whichever is longer. These documents should be maintained, stored securely and backed up.

- In the scenario where ePHI is involved, the state or the jurisdiction may require additional document retention period.

Issue Specific Security Policy.

While working with private medical data (ePHI), the organization which resides within the United States of America, must follow the HIPAA Standards. Hence, the disposal and sanitation of unused devices and media is an important issue to be addressed.

A few policies that address this specific issue of disposal of unused media are mentioned below:

[1] Using correct disposal methods (paper records).

- For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

- Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area.

[2] Having a disposal vendor.

- A new disposal vendor/organization should be appointed as a business associate to pick up and shred or destroy the PHI.

[3] Using correct disposal methods (software records).

- For PHI on electronic media, clearing, purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media: melting, incineration.

Systems Specific Security Policy.

[1] Daily mandatory MySQL port scans.

- The Open Dental Software uses the MySQL server for storage of sensitive patient data.

- MySQL server uses the port 3306 by default. This port should not be accessed from a host outside the organization.

- A guideline should be in place for the data handlers to check the default port daily and after large read/write tasks.

- Tools as or similar to ‘Network Mapper’ should be leveraged. A simple way is to run the `server_host 3306` command on the host where the MySQL server is installed. Where, `server_host` is the host name or the IP address of the trusted host where MySQL server runs.

- After running the command, if the telnet connection hangs up or is refused, it indicates that the port is blocked. This is the ideal result.

- If after running the above command a connection is open and some garbage values are obtained, this indicates that the port is open. In such cases, the port should be closed on the firewall or router.

Business Continuity Plan.

During an unplanned disruption or obstruction of service, a Business Continuity Plan offers instructions on what to do and how to operate. The following are the business continuity plans points for the 'Open Dental Software'.

Have you documented in your policies and procedures various emergency types and how you would respond to them?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How does your practice prevent, detect, and respond to security incidents?	All of the above.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?	Written and verbal communication as well as coordinated corrective action planning.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.Written results of the risk assessment should be communicated to the personnel responsible for responding to identified threats and vulnerabilities. The responsible persons should be involved in the creation of corrective action plans to mitigate threats and vulnerabilities for which they are responsible.

Do you make sure that information security and risk management documentation is available to those who need it?	Yes. Documentation is made available to appropriate workforce members in physical and/or electronic formats (for example, our practice's shared drive or intranet).	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you ensure that security and risk management documentation is available to those who need it?	Appropriate workforce members receive instruction on our information security documentation and where to find it as part of their periodic privacy and security training. Documentation is securely made available to workforce members in physical or electronic formats.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Has your practice evaluated and determined which systems and ePHI are necessary for maintaining business-as-usual in the event of an emergency?	Yes, we have a process of evaluating all hardware and software systems, including those of business associates, to determine criticality of the systems and ePHI that would be accessed by executing our contingency plan. This is documented along with our asset inventory.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you have a plan for backing up and restoring critical data?	Yes, we have a plan for determining which data is critically needed, creating retrievable, exact copies of critical data and how to restore that data, including from alternate locations. We also test and revise the plan, as needed.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How is your practice's emergency procedure activated?	Upon identification or initiation of an emergency situation, emergency procedures are activated according to documented procedure, such as by formal communication from the security officer or other designated personnel.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

How is your emergency procedure terminated after the emergency circumstance is over?	Upon the conclusion of the emergency situation, normal operations are resumed according to documented procedure, such as by formal communication from the security officer or other designated personnel.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Who within your practice is responsible for developing and implementing information security policies and procedures?	The security officer is a member of the workforce identified by name in policy documents.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you identify and document the role and responsibilities of the security officer?	Yes. The security officer is identified by role and this is documented in our practice's information security policies, which describes the role's responsibilities.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Is your security officer qualified for the position?	Yes. The security officer is an assigned member of the workforce familiar with security and has the ability to design, implement, and enforce security policies and procedures.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do workforce members know who the security officer is?	Yes. Workforce members are aware of who our security officer is.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do workforce members know how and when to contact the security officer?	Workforce members are made aware of the identity of the security officer and reasons for contacting the security officer as part of their orientation to the practice (upon hire) as well as periodic reminders of our internal policies and procedures (e.g. periodic review).	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Contingency Plan.

The contingency plan is a set of instructions or a course of action to be taken to assist on organization, on how to respond to certain events. These plans are also known as 'Plan B', since these are the actions to be performed, when the originally planned tasks fail.

The following is the contingency planning summary for the 'Open Dental Software'. The SRA Tool is used to develop the contingency plan report.

Areas of Success (100%)		
Does your practice have a contingency plan in the event of an emergency?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Is your contingency plan documented?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you periodically update your contingency plan?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you ensure that your contingency plan is effective and updated appropriately?	We periodically review the plans contents, perform tests of the plan, and record the results. We revise the plan as needed and document this in policy.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Have you considered what kind of emergencies could damage critical information systems or prevent access to ePHI within your practice?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
What types of emergencies have you considered?	All of the above.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Have you documented in your policies and procedures various emergency types and how you would respond to them?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Does your practice have policies and procedures in place to prevent, detect, and respond to security incidents?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How does your practice prevent, detect, and respond to security incidents?	All of the above.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Has your practice identified specific personnel as your incident response team?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

How are members of your incident response team identified and trained?	Workforce members are trained on their role and responsibilities as part of the incident response team (upon hire) as well as periodic reminders of our internal policies and procedures and testing exercises.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Has your practice evaluated and determined which systems and ePHI are necessary for maintaining business-as-usual in the event of an emergency?	Yes, we have a process of evaluating all hardware and software systems, including those of business associates, to determine criticality of the systems and ePHI that would be accessed by executing our contingency plan. This is documented along with our asset inventory.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How would your practice maintain access to ePHI in the event of an emergency, system failure, or physical disaster?	We have established procedures and mechanisms for obtaining necessary electronic protected health information during an emergency.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

How would your practice maintain security of ePHI and crucial business processes before, during, and after an emergency?	We have robust contingency plans which provide for alternate site or other means for continued access to ePHI. We test them periodically to ensure continuity of security processes in an emergency setting.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you have a plan for backing up and restoring critical data?	Yes, we have a plan for determining which data is critically needed, creating retrievable, exact copies of critical data and how to restore that data, including from alternate locations. We also test and revise the plan, as needed.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How is your practice's emergency procedure activated?	Upon identification or initiation of an emergency situation, emergency procedures are activated according to documented procedure, such as by formal communication from the security officer or other designated personnel.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

How is access to your facility coordinated in the event of disasters or emergency situations?	We have written policies and procedures outlining facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency. Members of the workforce who need access to the facility in an emergency have been identified. Roles and responsibilities have been defined. A backup plan for accessing the facility and critical data is in place.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

How is your emergency procedure terminated after the emergency circumstance is over?	Upon the conclusion of the emergency situation, normal operations are resumed according to documented procedure, such as by formal communication from the security officer or other designated personnel.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you formally evaluate the effectiveness of your security safeguards, including physical safeguards?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you evaluate the effectiveness of your security safeguards, including physical safeguards?	We have procedures in place to evaluate the effectiveness of our security policies and procedures, physical safeguards, and technical safeguards. Our evaluation is conducted periodically and in response to changes in the security environment.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Disaster Recovery Plan.

The Disaster Recovery Plan is a document which assists an organization or company to follow detailed steps on how to recover from a unplanned disaster like cyber-attacks, natural disasters etc.

The following is the disaster recovery plan summary for the 'Open Dental Software'. The SRA Tool is used to develop the disaster recovery report.

How is access to your facility coordinated in the event of disasters or emergency situations?	We have written policies and procedures outlining facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency. Members of the workforce who need access to the facility in an emergency have been identified. Roles and responsibilities have been defined. A backup plan for accessing the facility and critical data is in place.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How is your emergency procedure terminated after the emergency circumstance is over?	Upon the conclusion of the emergency situation, normal operations are resumed according to documented procedure, such as by formal communication from the security officer or other designated personnel.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Do you identify specific personnel to respond to and mitigate the threats and vulnerabilities found in your SRA?	Yes.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?	Written and verbal communication as well as coordinated corrective action planning.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.Written results of the risk assessment should be communicated to the personnel responsible for responding to identified threats and vulnerabilities. The responsible persons should be involved in the creation of corrective action plans to mitigate threats and vulnerabilities for which they are responsible.
Do you make sure that information security and risk management documentation is available to those who need it?	Yes. Documentation is made available to appropriate workforce members in physical and/or electronic formats (for example, our practice's shared drive or intranet).	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How would your practice maintain access to ePHI in the event of an emergency, system failure, or physical disaster?	We have established procedures and mechanisms for obtaining necessary electronic protected health information during an emergency.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

How would your practice maintain security of ePHI and crucial business processes before, during, and after an emergency?	We have robust contingency plans which provide for alternate site or other means for continued access to ePHI. We test them periodically to ensure continuity of security processes in an emergency setting.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Is protection from malicious software (including timely antivirus/security updates and malware protection) covered in your procedures?	Yes. Software protection is included in our procedures. This includes a review of our procedures for guarding against malware, and the mechanisms in place for protection, and how procedures for workforce members to follow can to detect and report malicious software.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Security Plans for Business Associates.

The 'Open Dental Software' stores medical data. Hence, as per the HIPAA standards of the United States of America, extra care and procedures are needed to be followed, when business associates are involved. These business associates usually include an external sanitization and disposal team, medical researchers etc.

Following are the planning points for the 'Open Dental Software', while working with external business associates.

Areas of Success (89%)		
Do you contract with business associates or other third-party vendors?	Yes.	Make sure all business associates and third-party vendors have been evaluated to determine whether or not they require a Business Associate Agreement.
How do you identify which business associates need access to create, receive, maintain, or transmit ePHI?	We review business associate contracts to determine which vendors or contractors require access to ePHI and we include a Business Associate Agreement (BAA) in our contract with them.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How does your practice enforce or monitor access for each of these business associates?	We determine degree of access based on the amount of ePHI accessed, the types of devices or mechanisms used for access, and our ability to control and monitor third-party access.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do business associates communicate important changes in security practices, personnel, etc. to you?	Our BAAs include language describing how security-relevant changes should be communicated to our organization.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

Have you executed business associate agreements with all business associates who create, receive, maintain, or transmit ePHI on your behalf?	Yes. We ensure all business associates have a fully executed BAA with us before creating, receiving, maintaining, or transmitting ePHI on our behalf.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How do you maintain awareness of business associate security practices? (e.g. in addition to Business Associate Agreements)	Our practice performs extra due diligence in the form of monitoring third-party connections to our information systems or other forms of access, in addition to including language for security compliance in our Business Associate Agreements (BAAs).	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
How does your practice document all of its business associates requiring access to ePHI?	We maintain a current listing of all business associates with access to ePHI in addition to having Business Associate Agreements (BAAs) on file with any business associates with access to ePHI.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.
Do you obtain Business Associate Agreements (BAAs) from business associates who access another covered entity's ePHI on your behalf?	Yes. We make sure to have BAAs in place with covered entities for which we are Business Associates as well as subcontractors to those covered entities who contract with us.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

The following is addressed, assuming that the organization does not allow third-party access to the ePHI currently.

Areas for Review (11%)		
Do you allow third-party vendors to access your information systems and/or ePHI?	No.	Working with business associates and third-party vendors can be beneficial to your practice, as long as reasonable and appropriate security precautions are taken for business associates accessing ePHI.

Security/Organizational Risks and Vulnerabilities.

The risks and vulnerabilities of the 'Open Dental Software' will be discussed in this section. The SRA Tool helped identify the associated risks with this software. The four vulnerabilities will be stated, and their defense plans will be emphasized further in the study.

Main vulnerabilities/risks:

[1] Inappropriate disposal and sanitation of unused devices.

[2] Insufficient rules for third party vendor access.

[3] MySQL protection.

[4] Untrustworthy employee or business associate.

⚠ Risk [1] Inappropriate disposal and sanitation of unused devices and PHI.

Section 5, Security and the Practice	Risk Score: 4 %
Threats & Vulnerabilities	Risk Rating
Inadequate sanitation of media	
Information disclosure or theft (ePHI, proprietary, intellectual, or confidential)	High
Disclosure of passwords and or login information	High
Unauthorized access to ePHI/sensitive information	High
Unknown disposition of unused devices and data	High
Unauthorized modification of user accounts and/or permissions	High

⚠ **Risk [2] Insufficient rules for third party vendor access.**

Areas for Review

Q2. Do you allow third-party vendors to access your information systems and/or ePHI?

Your Answer: No.

Education: Working with business associates and third-party vendors can be beneficial to your practice, as long as reasonable and appropriate security precautions are taken for business associates accessing ePHI.

⚠ **Risk [4] Untrustworthy employee and business associate.**

Section 3, Security & Workforce		Risk Score: 5 %
Threats & Vulnerabilities		Risk Rating
Untrustworthy employee or business associate		
	Information disclosure (ePHI, proprietary, intellectual, or confidential)	Medium
	Disruption of business processes or information system function	Medium
	Sensitive data exposed or tampered with by insider	High
	Misuse of information systems and/or hardware	High
	Falsification or destruction of records and/or data corruption	High
	Unauthorized access granted to outsiders	High

Defense Plans for the risks/vulnerabilities.

⚠ Risk [1] Inappropriate disposal of unused devices and PHI.

✅ **Using correct disposal methods (paper records).**

- For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

- Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area.

✅ **Having a disposal vendor.**

- A new disposal vendor/organization should be appointed as a business associate to pick up and shred or destroy the PHI.

✅ **Using correct disposal methods (software records).**

- For PHI on electronic media, clearing, purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media: melting, incineration.

⚠ **Risk [2] Insufficient rules for third party vendor access.**

✅ **Plan a Business Associate Agreement.**

- Both the organizations should be under a Business Associate Agreement, if PHI is shared to a third-party vendor or a research team.

- Should be signed by the business associate, before handling the PHI.

- If a security breach occurs and the PHI is exposed, the BAA contract should clearly hold one party responsible.

✅ **Changing the frequency of data.**

- Some PHI data handed to the research team is cleared, masked or changed. This may prove to be not helpful to conduct research.

- Changing the frequency of the data can help maintain the privacy of the patients as well as conducting good data analytics.

- While performing analysis, the original data numbers (specific) are not helpful. The correlation between the numbers is more important.

Original data.

Patient_name	Patient 1	Patient 2	Patient 3	Patient 4
Age	22	25	26	29

Reconstructed data.

Patient_name	Patient 1	Patient 2	Patient 3	Patient 4
Age	27	30	31	34

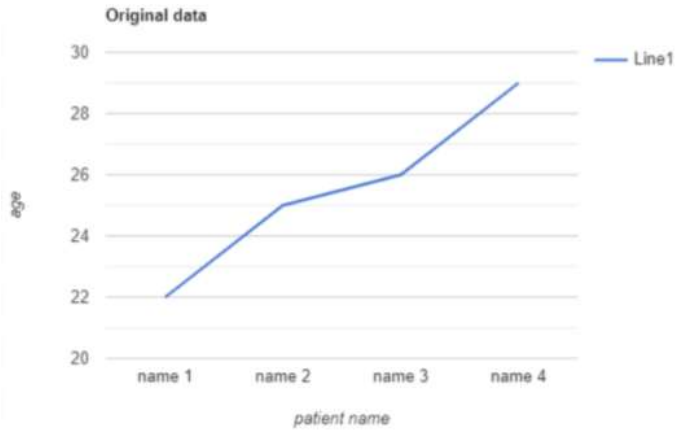
The entire original data can be transformed by a different percentage.

- Changing the frequency of the data.

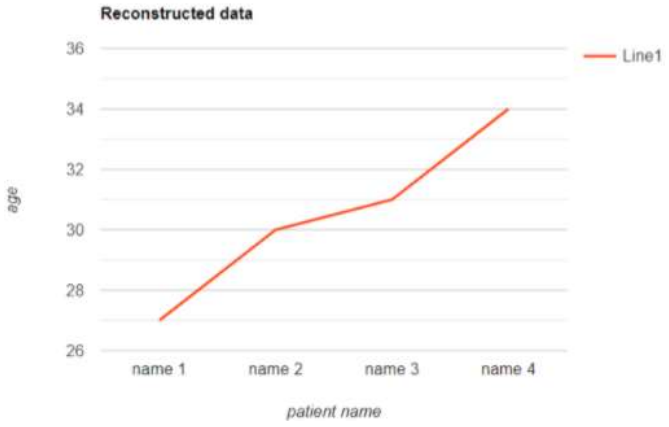
Formula for the percentage change.

$$\text{percent change} = \frac{\text{final} - \text{initial}}{|\text{initial}|} \times 100$$

- To revert back to the original data, the healthcare employees can maintain an encrypted file which contains the ‘percentage change key’.



Line graph for the original data.



Line graph for the reconstructed data.

As seen above, the line graphs for both original and reconstructed data is similar. This may help the patient’s privacy to be preserved and also the research team can perform successful data analytics.

⚠ Risk [3] MySQL protection.

✅ Database Replication.

- Replication is a technology built into MySQL that continuously keeps a slave database synchronized with its master database.

- The OpenDentImages (database folder for Open Dental Software) should be kept synchronized.

✅ Multi-tenant Hosting.

- Having a separate virtual machine with its own:

1) MySQL instance.

2) OpenDentImages folder (Open Dental Software's database folder)

Hence, easy disaster recovery after a MySQL injection attack occurs, since the VM can be moved to a different server.

⚠ Risk [4] Untrustworthy employees.

✅ Perform stringent background checks.

- While hiring, the background checks should include contacting previous employers, Google searches, and checking the employee's social media accounts.

✅ Monitor employee activity.

- In a healthcare environment it is rather difficult to differentiate between legitimate data access and harmful actions. HIPAA requires PHI access logs to be maintained and regularly checked.

✅ Encrypt PHI on all portable devices.

- Portable electronic devices can easily be stolen, but the theft of a device need not result in the exposure of PHI.

References.

[1] SRA-Toolkit (nih.gov)

[2] The Security Rule | HHS.gov

[3] Open Dental Software - Open Source Practice Management