



Supervision Assist

HIPAA Safeguards & Best User Practices



Contents

- Introduction2
- 1. Data Protection in Supervision Assist3**
 - 1.1 User & Client Data3
 - 1.2 HIPAA BAA.....3
 - 1.3 HIPAA Safeguards3
- 2. Electronic Protected Health Information (ePHI) in Supervision Assist4**
 - 2.1 Activity Log4
 - 2.2 Live Sessions5
 - 2.3 Clients7
 - 2.4 Evaluations & Forms8
- 3. Additional User Best Practices9**
 - 3.1 SA Account Security.....9
 - 3.2 Computer Security9
 - 3.3 Client Privacy & Confidentiality.....10
- 4.0 Data Breach11**
 - 4.1 Definition11
 - 4.2 Your Responsibility in a Suspected Data Breach11
 - 4.3 Our Response to Data Breaches12

Introduction

Supervision Assist (SA) is used in your practicum and internship with real clients who are legally protected by FERPA and HIPAA rules and regulations. As you work in SA, you may encounter scenarios where ePHI (Electronic Protected Health Information) must be entered or uploaded and, although SA is a highly secure system, it is recommended that you minimize the instances of ePHI.

For your peace of mind as well as your clients', your university's, and ours at SA, we have built this document to outline our application's HIPAA security, inform you of areas in SA that can contain ePHI and recommend important best practices.

1. Data Protection in Supervision Assist

1.1 User & Client Data

- All data that is entered or uploaded in SA by trainees, university staff, or related program partners (e.g. supervisors) is safely stored and replicated in encrypted AWS servers.
- All data is transmitted through encrypted channels using the latest TLS standards.
- Data containing ePHI (e.g. uploaded client files or live session recordings) is purged according to defined schedules based on your university's policies.
- All stored data, whether being transmitted or stored, is handled with the same high security level in transit and at rest.

1.2 HIPAA BAA

SA requires BAA (Business Associate Agreement) contracts from all sub-contractors in order to ensure that sub-contractors and other third parties handle the data in SA with utmost care.

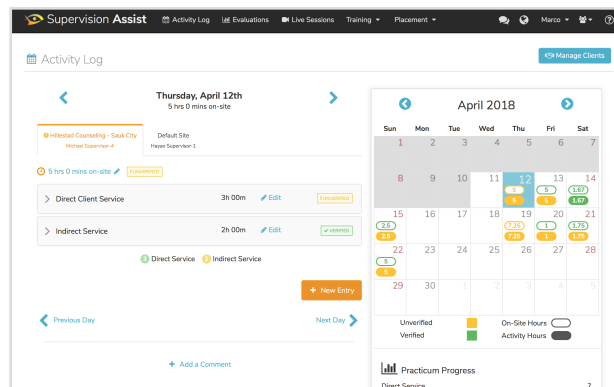
1.3 HIPAA Safeguards

- **Automatic Logoff:** Sessions are terminated after 10 minutes of inactivity.
- **Upload Controls:** Supervisors can set permissions on a per-trainee basis to allow or prevent uploading sensitive files, as well as view what is being shared.
- **Risk Analysis & Management:** SA is secured against anticipated attacks, impermissible uses, and known threats.
- **Physical Safeguards:** Access management prevents unnecessary access to production data.
- **Disposal:** Uploaded files during the course of training in SA are safely disposed of upon graduation.

2. Electronic Protected Health Information (ePHI) in Supervision Assist

2.1 Activity Log

Activity Log entries offer trainees the option to associate an entry with a client, as well as to enter session notes in the Journal.



Safeguards

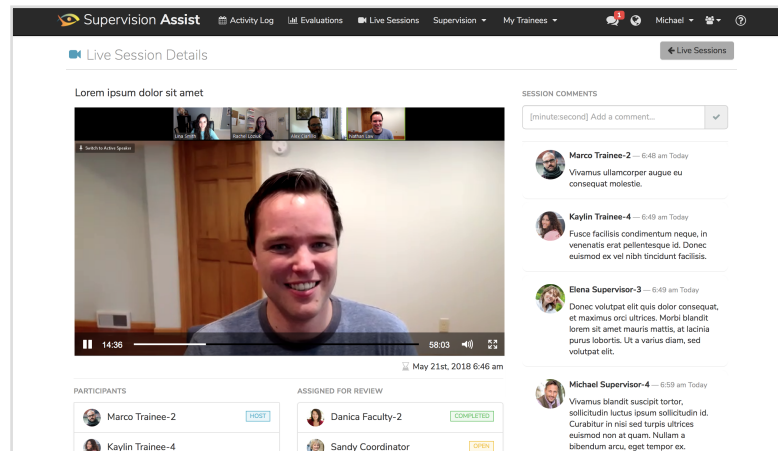
- Supervisors can only view Activity Log entries created by the trainees they are supervising at their site.
- Entries and notes are encrypted and scrambled so that only the trainee, the faculty supervisor, program coordinator, and site supervisor can read them.

User Best Practices

- If adding a client to the entry, the New Client modal explicitly advises against using client names; clients should be assigned "codes" that only you and your supervisor would know.
- The Journal instructions explicitly advise against including client names or any other personally-identifying information in the notes; although secured, do not enter any sensitive information in the Journal.
- Apply the above-described level of care and sensitivity in your every day use of SA and the Activity Log.

2.2 Live Sessions

Live Sessions are particularly private sets of data requiring the utmost level of caution and security, because they can contain the most ePHI (e.g. the client's face, voice, and personally-identifying details in conversation). This applies to real-time, cloud-recorded, and uploaded Live Sessions.



Safeguards

- Live Sessions are encrypted in real-time and only allow those listed as participants to partake (or listen in on) the session.
- Live Sessions are only shared with participants of the live session, or registered users who have been granted access.
- Live Session recordings can not be downloaded, and are encrypted on the Supervision Assist servers.

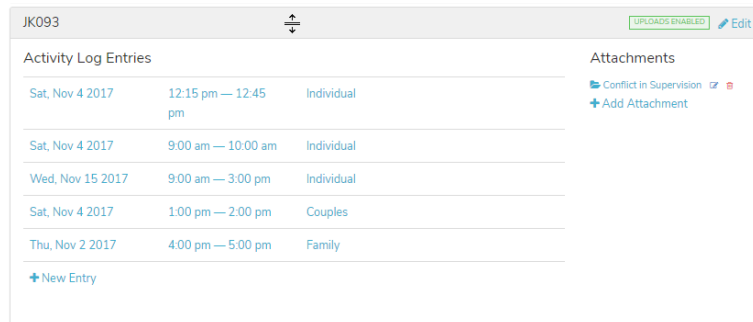
User Best Practices

- Ensure you are in a physically secure and private location when hosting or participating in a Live Session.
- Always obtain written permission from clients prior to recording, and ensure they are aware when being recorded.
- A recorded or uploaded Live Session can be shared with non-participants by assigning it as a Task; never share a session recording by sending an actual video or audio file, especially in unsecured mediums like email.

- Always obtain permission from your site supervisor prior to sharing a recorded Live Session with other users in SA.
- Take special care to only share client sessions with those who have permission to review these sessions and who can stream these recordings in physically secure and private locations; likewise if a Live Session is shared with you.
- If you create a Live Session by uploading an audio or video file that was recorded outside of SA, do not leave your computer unattended while the upload is taking place. Once completed, it is critical that you delete your local copy of the file.

2.3 Clients

Similar to Activity Log entries, trainees can also add clients in the dedicated Clients page, which also lists associated entries (if any) for each client.



The screenshot shows a web interface for a client named JK093. At the top right, there is a green box that says "UPLOADS ENABLED" and an "Edit" link. Below this, there are two main sections: "Activity Log Entries" and "Attachments".

Activity Log Entries		
Sat, Nov 4 2017	12:15 pm — 12:45 pm	Individual
Sat, Nov 4 2017	9:00 am — 10:00 am	Individual
Wed, Nov 15 2017	9:00 am — 3:00 pm	Individual
Sat, Nov 4 2017	1:00 pm — 2:00 pm	Couples
Thu, Nov 2 2017	4:00 pm — 5:00 pm	Family

At the bottom of the Activity Log Entries section, there is a link that says "➕ New Entry".

The Attachments section on the right contains a blue icon, the text "Conflict in Supervision", a checkmark icon, and a red square icon. Below this, there is a link that says "➕ Add Attachment".

Safeguards

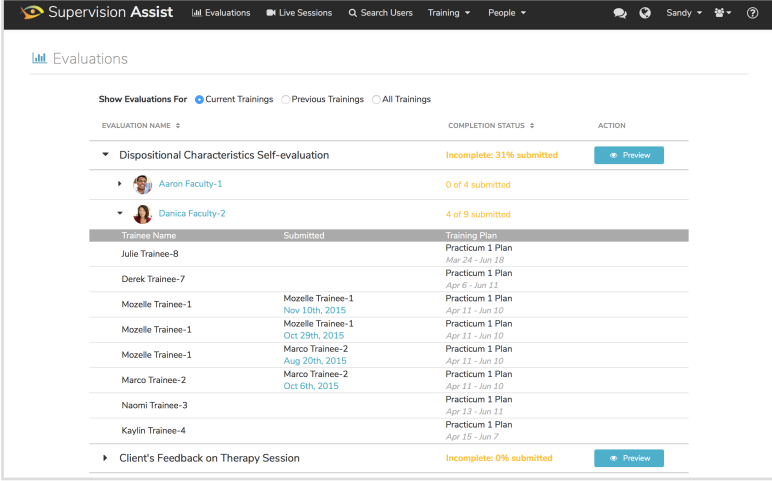
- Site supervisors can control whether or not their trainees can upload client-related files via 3 options:
 - **Automatically Enabled:** Trainees can upload data linked to any/all of their clients without needing explicit permission.
 - **Per-Client Request:** Trainees must request permission from their supervisor to upload data for each client.
 - **Automatically Disabled:** Trainees are not allowed to upload data for any/all of their clients, and they cannot request permission to upload.

User Best Practices

- Any files that contain sensitive information should be uploaded (or not uploaded) based on the above permissions; do not upload or attach these files anywhere in SA that is not designated for sensitive information.
- If you do have permission to upload client data, it is critical that you delete your local copy of the file once it has been successfully added to SA, and do not leave your computer unattended while the upload is taking place.
- If you wish to review previously-uploaded files after deleting your local copy, ensure that you do so in a physically secure and private location.

2.4 Evaluations & Forms

Evaluations and agreement forms can contain ePHI, depending on your university's requirements, and care must be taken to keep this data safe.



Supervision Assist | Evaluations | Live Sessions | Search Users | Training | People | Sandy

Evaluations

Show Evaluations For Current Trainings Previous Trainings All Trainings

EVALUATION NAME	COMPLETION STATUS	ACTION
Dispositional Characteristics Self-evaluation	Incomplete: 31% submitted	Preview
▶ Aaron Faculty-1	0 of 4 submitted	
▶ Danica Faculty-2	4 of 9 submitted	
Trainee Name	Submitted	Training Plan
Julie Trainee-8		Practicum 1 Plan Mar 24 - Jun 18
Derek Trainee-7		Practicum 1 Plan Apr 6 - Jun 11
Mozelle Trainee-1	Mozelle Trainee-1 Nov 10th, 2015	Practicum 1 Plan Apr 11 - Jun 10
Mozelle Trainee-1	Mozelle Trainee-1 Oct 29th, 2015	Practicum 1 Plan Apr 11 - Jun 10
Mozelle Trainee-1	Marco Trainee-2 Aug 20th, 2015	Practicum 1 Plan Apr 11 - Jun 10
Marco Trainee-2	Marco Trainee-2 Oct 6th, 2015	Practicum 1 Plan Apr 11 - Jun 10
Naomi Trainee-3		Practicum 1 Plan Apr 13 - Jun 11
Kaylin Trainee-4		Practicum 1 Plan Apr 15 - Jun 7
▶ Client's Feedback on Therapy Session	Incomplete: 0% submitted	Preview

Safeguards

- All forms are secured in SA using HIPAA requirements for security during transmission and when in storage.
- Evaluations are configured for granular settings, such as only allowing specific roles to review answers.
- Depending on the university's needs, some evaluations can request information about clients which can result in ePHI; in this case, you must ensure that you have obtained permission to do so from your site supervisor and your client.

User Best Practices

- If a form asks you to enter any client ePHI make sure you have the proper authorization from you Site Supervisor and client.

3. Additional User Best Practices

3.1 SA Account Security

- Use a unique password for authenticating into SA; do not include your email, name, date of birth, or any other text that can be linked to your credentials.
- Do not share your password with anyone, for any reason.
- The longer your password is, the more secure it will be; if you are worried you might forget such a password, consider using a 3rd-party password manager to safeguard your credentials.
- Because internet browsers can significantly affect security, we require users to access SA with one of the browsers listed below. All Internet Explorer versions are not well secured and therefore unsupported.

Recommended browsers:

- Chrome 64+
- Firefox 58+
- Edge 40+
- Safari 10+

Default browsers in the following systems:

- Windows 8 or higher
- Mac 10.9 (Mavericks) or higher
- iOS (iPhone/iPad) 9+
- Android 6+ (Marshmallow)
- Linux equivalent to Ubuntu 14.04 (Trusty) or higher

3.2 Computer Security

- Keep your computer and its contents inaccessible to unauthorized users by setting it to require a password to unlock.
- Do not leave your computer unattended in a public place without locking your screen first (and having a password requirement to unlock it).
- To protect your data in the event of a theft, be sure to encrypt your computer's hard drive in addition to setting a password to unlock it.
- Configure your system to auto-lock and require a password after 10 minutes of inactivity.

- Regularly scan and protect your computer from viruses, malware, and spyware which can compromise your personal information and your clients'.

3.3 Client Privacy & Confidentiality

- Obtain clients' written, signed, and dated authorization for release of information to named parties prior to uploading client ePHI to SA.
- Talk with your supervisor about acceptable levels of ePHI (if any) to have in SA, and identify clearly where/when ePHI may be used.
- Be sensitive to the client's right to privacy and avoid adding ePHI where it isn't necessary; in Activity Log entries, carefully consider whether or not ePHI is relevant to your Journal notes.
- Do not view files, recordings, or pages containing ePHI in public locations if the information can be seen, overheard, or read by a passerby.
- Before using public WiFi internet, be sure to connect to a reputable VPN service that can protect your data from being intercepted.

4.0 Data Breach

4.1 Definition

A breach of Protected Health Information (PHI) is defined as the acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by HIPAA, which poses a significant risk of financial, reputational, or other harm to the affected individual.

4.2 Your Responsibility in a Suspected Data Breach

The following are the most likely events that can lead to a data breach of PHI, so it is important that you are aware of how you can prevent such an incident.

1. **Unauthorized user accessing your account:** This would most likely be the result of (1) leaving your computer unprotected and unlocked in a public place, (2) using public computers and walking away without properly ending your session, or (3) having your login credentials stolen due to being unprotected.
2. **Unauthorized viewing of client PHI:** If you are viewing, reading, or listening to information that may contain ePHI in a location where the information can be seen or heard by others, this may constitute a data breach.
3. **Data left in an insecure location:** If information has been transcribed or files uploaded to SA, you are responsible for safely securing or destroying redundant copies of this information in order to minimize the risk of data being breached.

In the event of a data breach, you must immediately contact your program coordinator, your site supervisor, and alert us about the breach by emailing help@supervisionassist.com with the following information:

1. Subject line: *HIPAA Security Breach*
2. *Contact Information*
3. *Information about the Breach: Date, time, location of the breach, and a brief summary of events*

4.3 Our Response to Data Breaches

The most likely events that may result in a data breach of information in Supervision Assist are included in the Risk Analysis & Management section of our HIPAA documentation.

In order to comply with HIPAA's Privacy and Security Rules, it is the policy of Supervision Assist to mitigate known harm from an improper disclosure of Protected Health Information (PHI/ePHI) when it is practicable to do so.

Whenever we learn of harm caused by an improper disclosure of PHI, including electronic Protected Health Information (ePHI), we will take reasonable steps to mitigate the harm. We will take these steps whether the improper disclosure was made by us or by one of our business associates.

Discovery of a Breach

Supervision Assist will ensure that all incidents, threats, or violations that affect or may affect the privacy, confidentiality, integrity, or availability of PHI will be reported and responded to by our Chief Technical Officer, Chief Operating Officer and Business Manager

The three individuals above comprise the **Supervision Assist Privacy and Security Incident Response Team (IRT)**. The **Supervision Assist IRT** is charged with the responsibility of identifying, evaluating and responding to privacy and security incidents.

A breach will be treated as discovered as of the first day the breach is known or by exercising reasonable diligence would have been known.

Data Breach Procedures

Our Supervision Assist IRT will determine what specific steps are appropriate to mitigate particular harm. It is our policy to tailor mitigation efforts to individual harm.

Examples of some mitigation steps include: (1) Contacting the person(s) who obtained or observed the information (if possible) and obtaining Protected Health Information that was improperly disclosed and arranging permissible destruction of the data

improperly obtained. (2) Preventing further disclosure through agreements with the recipient.

If a breach has occurred, Following the discovery of a breach of unsecured PHI, the Supervision Assist IRT will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

Data Breach Notifications

Supervision Assists IRT will provide the required notifications without unreasonable delay and in no case later than 48 hours after discovery of a breach.

A notification will be provided to each individual affected by the discovered breach. The notification will include the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the Supervision Assist IRT is doing to investigate the breach, to mitigate harm to patients, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Written notification will be provided by email and phone call (where possible) to impacted parties.