VITALA

Technical Consultation for Safeguarding and Cybersecurity for Digital Comprehensive Abortion Care Tools in Latin America

MEETING REPORT

Background

Development of digital comprehensive abortion care programs have accelerated especially since the Covid-19 pandemic, though importantly these innovations preceded the pandemic. These initiatives include but are not limited to telemedicine, mobile applications, chatbots, hotlines, web-based programs with online support and any combination of these. These tools range from being harm-reduction tools to providing direct service delivery.

In Latin America specifically, various models of comprehensive abortion care have been implemented due to the legally restrictive contexts. More than 97% of women of reproductive age in Latin America and the Caribbean live in countries with restrictive abortion laws[1]. **However, there are a number of international, regional and national sexual and reproductive health organizations and grassroots colletives facilitating access to comprehensive abortion care. Given this context, by baseline there are safeguarding and risk mitigation strategies that must be in place to protect those doing the work and the individuals themselves.** The added layer of using digital means to provide care, requires us to also think about data storage, privacy and security of those involved.

Safeguarding broadly means preventing harm to people and the environment in which development and humanitarian assistance is delivered[2]. Safeguarding for digital comprehensive abortion care services requires a multi-facet approach to include considerations such as: protecting all those who are involved; ensuring that safeguarding is fully integrated into all stages of programme design, implementation, monitoring and review; incorporating safeguarding measures into digital communications/platforms; maintaining confidential reporting; and establishing appropriate referral pathways and feedback mechanisms.

Multiple organizations and abortion right advocates met on November 9th, 2021 to identify risk mitigation strategies and best safeguarding practices for digital abortion services provision (including telemedicine, chat support, AI, chatbots, apps, etc.) in legally restrictive settings, considering implications on users, providers, grassroots organizations and allies. **With the objective to co-create a best practices document to highlight the shared experiences of our organizations to build a safeguarding and program protection strategy adaptable to our respective scopes of work.**

The specific objectives for this consultation were:

- To bring together SRHR & Telehealth experts to identify best safeguarding practices for digital abortion services provision (including telemedicine, chat support, AI, chatbots, apps, etc.)
- To identify and share risk mitigation strategies for those who work in-country for our respective organizations, our allies and partner organizations and users themselves
- To highlight the key data security and privacy issues that must be considered to protect users and those who manage the digital platforms in legally restrictive settings

[1] https://www.guttmacher.org/sites/default/files/factsheet/ib_aww-latin-america.pdf
[2] https://safeguardingsupporthub.org/what-safeguarding

VITALA

Consultation outcomes

The consultation organizers (Vitala Global) compiled the information shared by participants based on four groups of interest: users, providers, allies and communities involved in the promotion of enabling environments for comprehensive abortion services, including information sharing and service delivery. These are the results of each working group:

Protecting the communities

This group was made up by prominent advocates from Venezuela and the region. They had an opportunity to share their experiences, and expertise, in implementing security and safeguarding practices and protocols in their respective organizations. We acknowledge the widespread fear (and existing risk) of criminalization among the Venezuelan participants. During the consult, they highlighted the risk of backlash when they become vocal about abortion rights or when their identities as advocates are public. However, there is also a sense of safety and protection when working and strategizing collectively. So, there is protective value when building partnerships and alliances.

Movement building is a way of creating support networks among advocates and community-based collectives, not only to provide referrals to users but to also build trust amongst one another. This collective work also prevents working in silos and expands the outreach organizations can have in historically marginalized communities. Working directly with communities might decrease the feeling of potential exposure and risk.

To address the risks of exposure and criminalization for community advocates, the recommendations shared by the group were:

1. Develop shared security protocols at interorganizational levels and partnership building. This might need strategies for sharing specific resources for safeguarding, clear communication channels, and agreements on how to face public events.
2. Harmonize existing digital security protocols and safeguarding practices among organizations and referral systems.
3. Emphasize the need and importance to invest resources in capacity-development and constant training in digital care and safeguarding for staff, volunteers, and collaborators.
4. Cultivate and maintain good relations with community members and leaders as it serves as a protection from external threats and as a way to find new and potential allies.
5. Develop and agree on daily practices of digital security. For example, a system of codes to avoid directly mentioning a specific language that is directly referring to abortion or self-managed abortion, or periodic elimination fo chat logs and messages, enable two-factor authentication.
6. Design emergency plans in case a threatening event occurs. For instance, know who will provide technical support to fix a security breach or who will provide legal assistance if needed.

VITALA

Protecting users

Supporting the ones who make the decision to terminate a pregnancy or not is at the core of our work, but it is a very personal space where there is one important risk involved: identities' exposure. It can be: the user's identity, or the provider's. In both cases, we must ensure that the security protocols are sufficient to prevent any leak of information coming from the user's devices or the provider's devices.

To address such risk, it was recommended to:

a. Save medical history to share amongst partners, or provider's information with a specific coding system or anonymize medical histories.
b. Have no backups in clouds, only users have access to the information they store in their Apps.
c. Have an alert mechanism for users to report potential threats or leaks.
d. Have restricted access to our platforms (2FA, periodic change of passwords)
e. Use encrypted platforms and comms channels with partners and team members.
f. Do a periodic erasure of data.
g. Have diverse VPN servers.

Protecting providers

Specific strategies to protect providers must be grounded in the national laws and regulations on data storage, if they exist in the context that we work with. The information that we keep to support user might put ourselves or our users at risk so it is recommended to:

1. Have a common understanding of the laws related to storage of medical data by providers.
2. Have a common glossary (or a coded logbook of services to aboid using abortion language), codes of conduct, and training for using safe language amongst providers.
3. Develop clear contracts with involved partners where we can specify how data will be stored and shared.
4. Set multi-factor authentication tools to log in.
5. Make sure that informed consenting is clear for users, specify if their data will be shared and what are their rights.
6. Have transparent monitoring systems in place and mechanisms to gather feedback in our working platforms.
7. Have proper VPN servers, choosing the server's where the state is going to be stored. So it's in countries where there are robust data protection laws in place.
8. Avoid tracking identifying information of the users.
9. Do a very clear data mapping from the onset of whenever we want to create platforms to link clients to service providers that we do map, very clearly, the data points that we anticipate will come from that connection.

Moreover, some of the platforms that might help to implement these activities are: Microsoft Dynamics CRM, Sharepoint, Teams Drive and Hetzner (a German cloud services).

VITALA

Protecting allies

With the limited time, the working group focused the discussion on the risks associated with the relationship with allies. It was evident that one group missing from the meeting were donors themselves as enough funding does not go towards safeguarding and cybersecurity protocols. It was acknowledged that being creative in our engagement as allies and utilizing our position to safeguard local teams can be very useful. The following key points came from the discussion:

1. Building the interventions but not having enough resources to safeguard their teams and services, not many grassroot organizations have access to resources for safeguarding and partnership building should include how resources will be shared to provide the services that we provide.
2. Scaling the interventions, there should be an additional risk management and mitigation strategy to safeguard users and allies involved in the service provision.
3. Differences with funders or donor's values and the nature of our work. This might be conflictive and an impediment to continue to implement our work.
4. The way we communicate with our donors can lead to misinterpretation of the information online. There must be a set memorandum of understanding or terms of how the information will be presented externally.
5. Censorship on social media: as we want to work with different populations, social media is a key space to reach out to them, to young people specifically. There must also be a way of safeguarding the people and allies who are publicly more vocal and open about abortion.

Consulta técnica para la salvaguarda y ciberseguridad de las herramientas digitales de atención integral del aborto en América Latina

INFORME DE LA REUNIÓN

Antecedentes

El desarrollo de programas digitales de atención integral del aborto se ha acelerado especialmente desde la pandemia de Covid-19, aunque lo importante es que estas innovaciones precedieron a la pandemia. Estas iniciativas incluyen, entre otras, la telemedicina, las aplicaciones móviles, los chatbots, las líneas de atención telefónica, los programas basados en la web con apoyo en línea y cualquier combinación de estos. Estas herramientas van desde la reducción de daños hasta la prestación directa de servicios.

En América Latina específicamente, se han implementado varios modelos de atención integral del aborto debido a los contextos legalmente restrictivos. Más del 97% de las mujeres en edad reproductiva en América Latina y el Caribe viven en países con leyes de aborto restrictivas . Sin embargo, hay una serie de organizaciones internacionales, regionales y nacionales de salud sexual y reproductiva, así como de colectivos de base, que facilitan el acceso a la atención integral del aborto. Teniendo en cuenta este contexto, por línea de base hay estrategias de salvaguardia y mitigación de riesgos que deben estar en su lugar para proteger a los que hacen el trabajo y los propios individuos. La capa añadida del uso de medios digitales para proporcionar atención, nos obliga a pensar también en el almacenamiento de datos, la privacidad y la seguridad de los implicados.

Salvaguardar significa, en términos generales, prevenir el daño a las personas y al entorno en el que se presta la ayuda humanitaria y al desarrollo . La salvaguardia de los servicios digitales de atención integral al aborto requiere un enfoque multifacético que incluya consideraciones como: proteger a todos los implicados; garantizar que la salvaguardia se integre plenamente en todas las etapas del diseño, la ejecución, el seguimiento y la revisión del programa; incorporar medidas de salvaguardia en las comunicaciones/plataformas digitales; mantener la confidencialidad de los informes; y establecer vías de derivación y mecanismos de retroalimentación adecuados.

Múltiples organizaciones y defensores del derecho al aborto se reunieron el 9 de noviembre de 2021 para identificar las estrategias de mitigación de riesgos y las mejores prácticas de salvaguardia para la prestación de servicios digitales de aborto (incluyendo la telemedicina, el soporte de chat, la IA, los chatbots, las aplicaciones, etc.) en entornos legalmente restrictivos, teniendo en cuenta las implicaciones para los usuarios, los proveedores, las organizaciones de base y los aliados. Con el objetivo de co-crear un documento de mejores prácticas para resaltar las experiencias compartidas de nuestras organizaciones para construir una estrategia de salvaguarda y protección de programas adaptable a nuestros respectivos ámbitos de trabajo.

Los objetivos específicos de esta consulta eran

- Reunir a expertos en SDSR y telesalud para identificar las mejores prácticas de salvaguardia para la prestación de servicios digitales de aborto (incluyendo telemedicina, asistencia por chat, IA, chatbots, aplicaciones, etc.)
- Identificar y compartir estrategias de mitigación de riesgos para quienes trabajan en el país para nuestras respectivas organizaciones, nuestros aliados y organizaciones asociadas y los propios usuarios
- Destacar los aspectos clave de la seguridad de los datos y la privacidad que deben tenerse en cuenta para proteger a los usuarios y a quienes gestionan las plataformas digitales en entornos legalmente restrictivos

Resultados de la consulta

Los organizadores de la consulta (Vitala Global) recopilaron la información compartida por los participantes en función de cuatro grupos de interés: usuarios, proveedores, aliados y comunidades implicadas en la promoción de entornos propicios para los servicios de aborto integral, incluyendo el intercambio de información y la prestación de servicios. Estos son los resultados de cada grupo de trabajo:

Proteger a las comunidades

Este grupo estaba formado por destacados defensores de Venezuela y de la región. Tuvieron la oportunidad de compartir sus experiencias, y conocimientos, en la implementación de prácticas y protocolos de seguridad y protección en sus respectivas organizaciones. Reconocemos el temor generalizado (y el riesgo existente) de criminalización entre los participantes venezolanos. Durante la consulta, resaltaron el riesgo de sufrir una reacción violenta cuando se manifiestan sobre el derecho al aborto o cuando su identidad como defensoras se hace pública. Sin embargo, también existe una sensación de seguridad y protección cuando se trabaja y se elabora una estrategia de forma colectiva. Por lo tanto, existe un valor de protección cuando se crean asociaciones y alianzas.

La construcción de movimientos es una forma de crear redes de apoyo entre los defensores y los colectivos de base comunitaria, no sólo para proporcionar referencias a los usuarios, sino también para crear confianza entre ellos. Este trabajo colectivo también evita el trabajo en silos y amplía el alcance que las organizaciones pueden tener en comunidades históricamente marginadas. Trabajar directamente con las comunidades puede disminuir la sensación de posible exposición y riesgo.

Para abordar los riesgos de exposición y criminalización de los defensores de la comunidad, las recomendaciones compartidas por el grupo fueron

1. Desarrollar protocolos de seguridad compartidos a nivel interorganizativo y de creación de asociaciones. Esto podría requerir estrategias para compartir recursos específicos para la salvaguarda, canales de comunicación claros y acuerdos sobre cómo afrontar los eventos públicos.
2. Armonizar los protocolos de seguridad digital existentes y las prácticas de salvaguarda entre organizaciones y sistemas de referencia.

3. Destacar la necesidad e importancia de invertir recursos en el desarrollo de capacidades y la formación constante en materia de cuidado y salvaguarda digital para el personal, los voluntarios y los colaboradores.
4. Cultivar y mantener buenas relaciones con los miembros y líderes de la comunidad, ya que sirve para protegerse de las amenazas externas y para encontrar nuevos y potenciales aliados.
5. Desarrollar y acordar prácticas diarias de seguridad digital. Por ejemplo, un sistema de códigos para evitar la mención directa de un lenguaje específico que se refiera directamente al aborto o al aborto autogestionado, o la eliminación periódica de los registros y mensajes de chat, habilitar la autenticación de dos factores.
6. Diseñe planes de emergencia en caso de que se produzca un evento amenazante. Por ejemplo, saber quién proporcionará apoyo técnico para solucionar una brecha de seguridad o quién proporcionará asistencia legal si es necesario.

Proteger a los usuarios

Apoyar a quienes toman la decisión de interrumpir o no un embarazo es el núcleo de nuestro trabajo, pero es un espacio muy personal en el que hay un riesgo importante: la exposición de las identidades. Puede ser: la identidad del usuario, o la del proveedor. En ambos casos, debemos asegurarnos de que los protocolos de seguridad son suficientes para evitar cualquier fuga de información procedente de los dispositivos de la usuaria o del proveedor.

Para hacer frente a ese riesgo, se recomendó:

1. Guardar el historial médico para compartirlo entre socios, o la información del proveedor con un sistema de codificación específico o anonimizar los historiales médicos.
2. No tener copias de seguridad en las nubes, sólo los usuarios tienen acceso a la información que almacenan en sus Apps.
3. Disponer de un mecanismo de alerta para que los usuarios informen de posibles amenazas o filtraciones.
4. Tener acceso restringido a nuestras plataformas (2FA, cambio periódico de contraseñas)
5. Utilizar plataformas y canales de comunicación encriptados con socios y miembros del equipo.
6. Haga un borrado periódico de los datos.
7. Tener diversos servidores VPN.

Proteger a los proveedores

Las estrategias específicas para proteger a los proveedores deben basarse en las leyes y reglamentos nacionales sobre el almacenamiento de datos, si existen en el contexto con el que trabajamos. La información que guardamos para dar soporte al usuario puede ponernos en riesgo a nosotros mismos o a nuestros usuarios por lo que se recomienda:

1. Tener un conocimiento común de las leyes relacionadas con el almacenamiento de datos médicos por parte de los proveedores.

2. Disponer de un glosario común (o un libro de registro codificado de los servicios para evitar el uso del lenguaje abortivo), códigos de conducta y formación para el uso de un lenguaje seguro entre los proveedores.
3. Desarrollar contratos claros con los socios implicados en los que podamos especificar cómo se almacenarán y compartirán los datos.
4. Establezca herramientas de autenticación multifactorial para iniciar la sesión.
5. Asegúrese de que el consentimiento informado sea claro para los usuarios, especifique si sus datos serán compartidos y cuáles son sus derechos.
6. Disponer de sistemas de seguimiento transparentes y de mecanismos para recabar opiniones en nuestras plataformas de trabajo.
7. Tener servidores VPN adecuados, elegir el servidor donde se va a almacenar el estado. Así que es en los países donde hay leyes de protección de datos robustos en su lugar.
8. Evitar el seguimiento de la información de identificación de los usuarios.
9. Hacer un mapeo de datos muy claro desde el principio de cada vez que queremos crear plataformas para vincular a los clientes con los proveedores de servicios que hacemos mapa, muy claramente, los puntos de datos que anticipamos que vendrá de esa conexión.

Además, algunas de las plataformas que podrían ayudar a implementar estas actividades son: Microsoft Dynamics CRM, Sharepoint, Teams Drive y Hetzner (un servicio alemán en la nube).

Proteger a los aliados

Con el tiempo limitado, el grupo de trabajo centró el debate en los riesgos asociados a la relación con los aliados. Fue evidente que un grupo que faltaba en la reunión eran los propios donantes, ya que no se destinan suficientes fondos a los protocolos de salvaguardia y ciberseguridad. Se reconoció que ser creativos en nuestro compromiso como aliados y utilizar nuestra posición para salvaguardar los equipos locales puede ser muy útil. Del debate surgieron los siguientes puntos clave:

1. Construir las intervenciones pero no tener suficientes recursos para salvaguardar sus equipos y servicios, no muchas organizaciones de base tienen acceso a recursos para la salvaguardia y la construcción de la asociación debe incluir cómo se compartirán los recursos para proporcionar los servicios que ofrecemos.
2. Al ampliar las intervenciones, debe haber una estrategia adicional de gestión y mitigación de riesgos para salvaguardar a los usuarios y a los aliados que participan en la prestación de servicios.
3. Diferencias con los valores de los financiadores o donantes y la naturaleza de nuestro trabajo. Esto podría ser conflictivo y un impedimento para seguir implementando nuestro trabajo.
4. La forma de comunicarnos con nuestros donantes puede llevar a una mala interpretación de la información en línea. Debe haber un memorando de entendimiento o términos establecidos sobre cómo se presentará la información al exterior.
5. Censura en las redes sociales: como queremos trabajar con diferentes poblaciones, las redes sociales son un espacio clave para llegar a ellas, a los jóvenes específicamente.

También debe haber una forma de salvaguardar a las personas y los aliados que son públicamente más vocales y abiertos sobre el aborto.