Tennessee Department of Health
HIV/STD Prevention Programs

Internet and Text Messaging
Policies and Procedures
2019

Table of Contents

Introduction

Partner notification plays an important role in STI control; and its practice must evolve with available technologies.

Internet-based Partner Services (IPS) is an all-encompassing term that refers to all partner services that can be provided through the internet, while Internet-based Partner Notification (IPN) refers to the specific activity of notifying partners of their possible exposure to a STI or HIV.

IPS should be used to augment traditional partner services. Partner locating information may be limited to a screen name from a social media account, dating/hookup app, website, or an email address making the internet the only viable option for providing partner notification (PN).

Objectives

These guidelines provide specific requirements on how the internet can be best used to conduct IPS in Tennessee. They have been developed as a response to the adaptation of internet technology by individuals joining new online sexual networks and the subsequent increase in disease transmission through these virtual communities. These instructions are based on Tennessee Department of Health (TDH) program experience, input from states, field experience from community-based organizations throughout the state, and recommendations from the Introducing Technology into Partner Services toolkit[1].

These tools are area specific and created for Tennessee to enhance the existing national guidelines; "National Guidelines for Internet-based HIV/STI Prevention: Accessing the Power of the internet for Public Health" [2] and to provide more guidance specifically crafted for Tennessee.

Compatibility with Tennessee Department of Health Policies

Any entity that conducts IPS must adhere to the existing TDH IPS Protocol and Guidelines and be willing and able to supply any and all supporting documentation. All staff must be fully trained and approved to conduct IPS prior to performing any portion of IPS.

> The TDH Human Resources has determined that DIS and supervisory staff participating in internet interventions would fall within official job duties as related to disease intervention, and are covered within the scope of the current *TDH Internet Usage Policy and the TDH Employee Confidentiality Policy*

[1] **Centers for Disease Control and Prevention. 2015.** *Introducing Technology into Partner Services: A Toolkit for Programs. Complete Report*

[2]**National Coalition of STD Directors. 2010. National guidelines for Internet-based STD and HIV prevention: Accessing the power of the internet for public health.**

Computer Security

Policies

Before conducting any internet interventions a written network security policy must exist. The goal of any network security policy is to reduce security risks. Firewalls, anti-virus, and backup strategies are some of the tools that can be used to help secure your network. A detailed security policy is a group of documents that make up the complete network security policy. For Tennessee, they include:

- Computer Acceptable Use - This document covers all computer access
- Password - Requirements for password protection
- Email - This policy covers the use of email
- Web – Specifications on what browsers may be used, configuration, and restrictions
- Remote Access –who can access what information from which locations (such as accessing work servers from home) and under what circumstances.
- Servers – a statement of the standard for servers

Confidentiality & Ethics

Confidentiality and purpose agreements such as the TDH *Internet-based Partner Services Computer and Technology Acceptable Use Agreement* (see Appendix A) must be signed by all staff performing IPS and by staff that may monitor operations, including Information Technology (IT) staff. Such agreements should include statements about the consequence of personal use of access passwords, e-mail addresses and agency profiles, as well as IT access to confidential emails or chats. Policies for managing improper use of computers and the internet must be established.

The personal use of any profile, webpage, email, or other work related tool that has been established for IPS will not be tolerated. All employees must establish and maintain a clear distinction between professional and personal internet usage.

Engagement of Key Stakeholders:

Important key stakeholders include, among others, the State Department of Health, the Information Technology Director, the Legal Department, agency management, persons who will conduct IPS, and HIV/STI program managers.

Ensuring that key stakeholders are informed and involved when appropriate will help to determine the success of your IPS program. Written communication delivered to patients through IPS at times instructs the patient to reach out to the IPS DIS supervisor to verify that the communication sent is factual. Verification by key stakeholders can expedite the time the partner takes in responding to the notification.

Internet-based Partner Services (IPS)

The emergence of the internet, social media, and dating/hookup apps as venues for initiating sexual contact has fostered the use of the internet for partner services. Internet-based Partner Notification (a task within the domain of Internet-based Partner Services) is the process of using the internet, social media, and dating/hookup apps to conduct or enhance the process of notifying persons of their potential exposure to an infectious disease. IPS should augment traditional methods of partner services, specifically provider referral, where appropriate. All current principles of partner notification apply to IPS.

The internet has contributed to syphilis outbreaks and rising STI rates (including HIV) across the country. Many of these cases have met for anonymous sex and the only information that may be known about the partner is a screen name, chat room profile, or email used to make the initial connection. When partner-locating information is limited to an e-mail address or screen name from a social network the use of the internet then becomes the only viable option.

Both the Division of STI Prevention & the Division of HIV Prevention at the U.S. Centers for disease Control & Prevention encourage the use of the internet for HIV/STI prevention including IPN. [3]

Staffing

All agencies that intend on conducting IPS must receive written approval by the TDH HIV/STI/Viral Hepatitis section. Staffing for IPS is dependent upon the program size, morbidity, and the appropriateness of using the internet for the target population.

Training

To be effective the appropriate staff members that are conducting IPS must be properly trained for all types of traditional partner services. The internet is constantly changing and new technologies continually emerge; therefore, DIS should be provided with ongoing training.

Training that is specific to the internet must be conducted to ensure that employees are able to direct the investigation and conduct the interviews around the original patients (also known as 'Client' or "Index Patient"). Staff conducting IPS must be familiar with the basic tools used to browse the internet and interact with others, such as web browsers, chat rooms, email, types of websites, social media, and dating/hookup apps. Knowledge of the terminology used in the various social networks and websites will help to assure a basic level of cultural competency (see the Glossary).

Surfing the internet should be an ongoing activity, as a variety of websites will be pulled into the process over time. It is also helpful to gather data on high-risk activities occurring in areas such as circuit parties, swinger clubs, cruising sites, raves, etc. This form of surveillance will help DIS to talk knowledgeably with their patients and will increase the options and resources for IPS related activities.

[3] **Walsh, C. July 13, 2010.** Dear Colleague Letter. Centers for Disease Control & Prevention, July 13, 2010.

Both new and experienced staff conducting partner services through the internet must have a full understanding of all guidelines, protocols, and procedures for conducting IPS. Recommended topics for training include:

- An overview of all national and state guidelines, protocols, and procedures regarding all aspects of Partner Services
- A review of the TDH Internet-based Partner Services Computer and Technology Acceptable Use Agreement
- Basics of the internet, including but not limited to;
    - Using links
    - Using a search engine
    - Website that can be used as tools for investigation
- Cultural competency training specifically geared towards online communities
- An overview of internet browsers such as Internet Explorer, Google Chrome and Firefox and how to use them, including but not limited to:
    - Using bookmarks
    - Entering in a URL (web address)
    - Printing web pages
    - History of sites visited
    - Searching web pages for key words
- The types and use of Email
- Completing forms and fields online
- Internet safety and personal privacy
- How to create a profile and upload a picture or logo

Supervision

All forms of partner services require quality assurance and monitoring but because IPS staff will have access to sexually explicit websites, particularly clear guidance must be given and regular monitoring must be conducted. Effective supervision will reduce the likelihood of error, help to demonstrate the program as effective, and reduce risks.

All DIS conducting IPS must be able to provide their supervisors with detailed documentation that includes a printing of correspondence sent and received. Correspondence will be reviewed for the quality of its content, any potential for future training, and to ensure professional boundaries are being maintained by the employee. All printed material, such as emails or any other printable correspondence, should accompany the field record.

When first establishing IPS, a log of all internet related activity that is being conducted by a DIS will be kept for a minimum of six (6) months and regularly reviewed by supervision. Consistent use of the Internet-based Partner Services Supervisory Website Log Sheet (see

Appendix J) during the adoption phase of IPS will ensure that supervision is aware of the time spent on the internet and the activities that are being conducted.

Before You Begin

Although internet interventions, such as IPS are similar to traditional partner services, differences do exist. The sexual nature of many communities within the internet, the potential for personal anonymity, and the possible risk to computer network security demand that careful attention be paid to issues such as cultural competency, computer security, and supervision.

Access to Sexually Explicit Online Sites

Unlike traditional settings, the internet provides access to a vast array of sexually explicit environments. Over 4.2 million pornographic websites exist, and it is estimated that 42.7% (approximately 72 million visitors) of all internet users view pornography online[4]. In addition to the large amount of pornography and number of adult oriented chat rooms, social networking sites focused on meeting for sex have proliferated often replacing the traditional meeting places such as bars and other public venues.

It can be anticipated that a significant portion of IPS will take place within an online adult community or through an adult oriented website. Because of the overtly sexual environments encountered within the internet, employees conducting IPS must be culturally competent, well prepared to view explicit content, thoroughly trained in how to best use the internet, social media, and dating/hookup apps for partner services, and properly supervised. Giving staff the ability to access sexually explicit websites may not be widely understood or initially recognized as a means of conducting disease intervention. Having the active participation and full support of all stakeholders will help to ensure that your IPS work is sanctioned, supported, and effective while dispelling any incorrect assumptions regarding the use of the internet for IPS.

Understanding Online Communities

Social interactions in online communities are varied and often complex. The characteristics of the people, the range of purposes they pursue, and the designs of the software supporting the website, social media platform, or app vary from community to community. Simply defined, an online community is 'a group of people, who come together for a purpose online, and who are governed by norms and policies' [5]

Online communities tend to take on the personality of their members; conversely, members will often adjust their personality or bring specific aspects of their personality to the forefront to conform to the social norms of the community that they are a member of. One person may join several different online communities in an effort to have different needs met. It is not unusual for a person to login to a site like Manhunt (where the focus is on seeking a

---

[4] **Preece, Jenny. 2000.** *Online Communities: Designing Usability, Supporting Sociability.* University of Maryland Baltimore County : John Wiley & Sons, 2000.

[5] **Ropelato, Jerry. 2008.** Internet Pornography Statistics. *TopTenREVIEWS.* [Online] 2008.

partner for sex) and conform to the norms within that community, while simultaneously maintaining a separate profile on a site such as Match.com where their intention may be to find a life partner. It is important to remember that a profile is simply a glimpse into one or more aspects of a personality and that a profile is created by an individual as a marketing tool with a specific purpose in mind (e.g. to engage in offline sexual activity, to seek a long term partner, or simply to expand their social circle).

The first step in understanding an online community is to review the marketing materials, the Frequently Asked Questions (FAQ), the images used, and the details of the exterior, such as the URL, the slogan, logo, and website design. A website's 'personality' may be reflected in the URL or in the name of the community. Websites with names like Manhunt, DaddyHunt, VeggieDate, SinglesWithScruples, and AdultFriendFinder reveal a great deal about their mission and the norms of the community they support. Since different sites attract different populations, a good IPS program will use a variety of sites.

Cultural Competency

Cultural competency is the capacity and skill to function effectively in environments that are culturally diverse and that are composed of distinct elements and qualities. Cultural competence begins with the HIV/STI professional understanding and respecting cultural differences. As with offline communities, internet communities will have their own 'culture'. Staff members that interact with Internet-based communities are expected to be culturally competent and skilled at communicating within the community they work.

Working in Online Venues

Due to the anonymity that online communities offer, individuals using the internet are free to adopt any identity they choose to create. Personal information and identifiers like sex, race, age, HIV status, or sexual orientation are self-disclosed and may be exaggerated or completely falsified.

This environment provides the perfect vehicle for individuals to act on impulses for which they may not otherwise have the opportunity. For example, an MSM may use online communities to act on sexual impulses with other men while remaining anonymous simply because they can take on a new identity though the internet, thus keeping their offline identity 'safe'.

Be aware that unlike traditional names, screen names and online identifiers can be changed easily and quickly. It is not unusual to lose a partner because of a changed screen name. It may be possible to track down a contact that has changed their screen name by reviewing profile information and pictures, but caution should be used.

In addition to the challenges that are faced with identity and anonymity, communication through the internet and within online communities presents unique challenges that are generally not encountered during face-to-face dialogue.

The fast paced and anonymous nature of the internet can also foster methods for communicating in ways that would generally not be acceptable in 'real world' social interactions. The social norms that govern how we communicate in public are significantly altered in online communities, especially networks that are centered on meeting for sex.

Communication in social networks designed around finding sex partners is often brief and to the point while being devoid of many of the social norms that exists in face to face communication. Emails between members of these communities are often incomplete sentences containing few words and may even be perceived as rude or abusive by an 'outsider'. When communicating electronically it is important to remember that this form of communication is devoid of the normal voice inflections or facial expressions and that these communities may have unique methods and ways of communicating.

As a person conducting IPS, the messages you send will most likely be outside of the community norms, structured in a more formal way, and void of any verbal clues to authenticate the message. Because of these unique issues found within online communities, the emails you send to contacts may at first be perceived as spam or a hoax. Spam (unsolicited email) and hoaxes are a fact of the internet. These annoying features of the virtual world exist within online communities as well. There are steps that can be taken that will help ensure that your message is delivered, these steps will be outlined later in this document.

When to Initiate IPS

Internet-based partner services may be initiated when there is insufficient locating or identifying information on a partner to conduct traditional disease intervention activities (e.g., name, address, phone number aren't known), but the index case can provide enough information to initiate contact through a website, email exchange, social media account, or dating/hookup app.

Roles and Responsibilities

The Initiating DIS Will:

- Elicit internet partner information from the Original Patient (OP), cut field records for these partners, and forward the field records (FR) to the IPS Supervisor for assignment.
- Be reassigned field records where the IPS DIS has obtained locating information.
- Work closely with IPS DIS to close field records.
- Close the OP's file when all partners' field records are closed.

The Supervisor Will:

- Reassign IPS field records to the IPS DIS.
- Supervise and perform quality control and assurance on all IPS activities.
- Serve as back-up DIS, if necessary.
- Maintain an IPS DIS work schedule.
- Maintain a log of times when logged into websites as directed.

The IPS DIS Will:

- Initiate IPS within one business day of notification.

- Review their voicemail and all website email accounts throughout the business day.
- Note all IPS activity in Notes section of PRISM and may also note on the FR.
- Reassign field records to the initiating DIS if locating information is obtained.
- Close or reassign field records within 7 days of last email sent.
- Ensure that their duties are properly covered by communicating with their supervisor to schedule vacation, sick, or personal time during. IPS DIS will have voicemail that indicates that the IPS DIS is out of the office and the replacement IPS DIS will be handling any communications.
- Maintain a log of times when logged into websites as directed.

IPS Documentation Requirements

- The employee will document all website activity on the "Internet-based Partner Services Website Log Sheet".
- The employee will complete a Field Record for the partner with all information pertaining to the internet partner (including physical descriptions, spelling of email addresses, sex venues, etc.) in PRISM. The employee then conducts IPS.
- The employee will document all IPS partner investigation activity in PRISM.
- The employee will archive each email partner's online profile as well as communication (both sent and received) and give proxy to the supervisor.
- Supervisor will review open and closed FRs and "Internet-based Partner Services Website Log Sheet."

Data Entry into PRISM

This section addresses contacts of infected individuals known by their screen names or email addresses only. This approach is based on how much information is available about a partner and serves as a systematic way to maintain accurate records of names, addresses, and phone numbers and screen names and email addresses. In this way, we can perform searches for individuals by their screen names and email addresses when no other information is available.

Internet partners are recorded as contacts of the OP; if a partner is not listed in PRISM (after a search using the FIRST NAME, LAST NAME, and AKA fields), a patient record is created for him/her.

PRISM data entry will follow this format:

Individuals who are only known by their screen name or email address should be entered into PRISM as an internet profile. Both the first and last names should be updated when more information becomes available. The screen names and locating websites should be added in the appropriate places. New screen names must be added as needed as individuals may change their screen names frequently.

FR dispositions will continue to follow current dispositions accepted by CDC.

Original Patient (OP) Interview

The use of the internet to provide partner services requires the same basic information needed to initiate a field investigation, which is a means to locate the individual. During the interview with the OP, questions that ask about websites that are being used to meet partners should be included (Appendix C). Just as in traditional partner services, the employee will gather as much information as possible regarding the characteristics of the partners in an effort to locate them. For each partner named, in addition to traditional identifying and locating information, information regarding websites, social media accounts, and dating/hookup apps visited, screen names, and email addresses of partners will be gathered and documented on interview and field records. When screen names and email addresses are the only locating information, DIS will record those as well as "**Internet**" in the "Other Identifying, Locating, or Medical Information" box of the Field Record.

If the OP is hesitant, it may help to show them the email that will be sent. It is important to stress that they will remain completely anonymous to their sex partners. The partner will not know who gave the employee the screen name and/or email address.

Having the exact spelling of screen names and email addresses is extremely important. Be aware that any physical descriptions that can be provided by the OP may assist in the confirmation of the screen name provided and may also be of assistance in locating the contact within the same website should they change their screen name.

Initiating Contact

Only staff members that have been officially designated and thoroughly trained in all aspects of traditional partner services and Internet-based partner services will carry out Internet-based Partner Notification.

E-mail Types

There are many types of email systems but in general, and for our purposes, email systems can be broken down into two categories: open and proprietary.

An 'open' email system includes web-based email (such as Hotmail, Yahoo!, or Gmail), Post office Protocol (POP3) and Internet Message Access Protocol (IMAP) email accounts. POP3 and IMAP accounts are usually provided with an internet account (such as Comcast or Verizon). Most email accounts provided with a domain (such as Microsoft or Health.State.NY.US) are also configured to be POP3 or IMAP accounts. Any system of electronic mail that is a system used by computers to send and receive messages transmitted from one computer to another outside of a single network can be considered an 'open' system. Email in an open system will pass through many computers throughout the internet before reaching its destination. An open email system may also be referred to as an "external" email system.

A 'proprietary' email system includes what can be termed as a 'closed' email systems such as found on websites like Manhunt, Adam4Adam, and AdultFriendFinder.com. Email within a closed system is sent and received on a proprietary or 'closed' network. Many of these systems do not use traditional email protocols (such as POP3) and are technically closer in design to Instant Messaging. Proprietary systems are often less costly to create, easier to

maintain, and require users to 'login' to read their mail, thus ensuring an increase in traffic for the website. Also called an 'internal' email system, proprietary email systems are password protected, requiring the user to login to authenticate their identity and gain access to all of the features of their account, including email.

Some websites, such as gay.com use a combination of proprietary and open systems. On gay.com each member has the option to use both an 'internal' and an 'external' email account with their membership. Members that are logged in to gay.com and use their profile to send email to another profile will use the internal or proprietary system. The recipient will receive the sent email within the website through their profile. When an email is sent via POP3 (using an 'open' system like Hotmail or Outlook) the email sent will be will be forwarded by gay.com to the email account that is associated with the screen name (the email address the user submitted during registration). The email address given at the time of registration is made up of their member's screen name with '@gay.com'.

Email IPN

IPN refers to the act of sending an email to a patient through the internet, and may or may not contain further information such as possible exposure to an infection or any HIV/STI related information.

A series of emails have been created to initiate IPN in a standardized manner (See Appendices H-N). These scripts are to be used when conducting IPS within a website's proprietary email system or when sending the email from a standalone client such as Microsoft Outlook. When sending email from a standalone client such as Microsoft Outlook, a legal disclaimer (as shown below) must be included at the bottom of each email.

> **CONFIDENTIALITY STATEMENT:** *This letter may contain confidential information belonging to the sender. If you are not the intended recipient or agent responsible for delivering this document to the intended recipient, you are hereby requested to immediately notify us. Any disclosure, copying, distribution or taking of any action about this letter is strictly prohibited by law.*

The rationale for the TDH IPS protocol is based on the fact that email is a secure form of communication with an individual. The following facts support this rationale:

- Anyone can register to create a free, secure, password-protected email account using multiple websites (e.g. Hotmail, Yahoo, AOL, Gmail, etc.).
- The majority of internet service providers (ISP) offer multiple accounts, each with secure password-protected email.
- In households that share an ISP, each member of the household will most likely have individual email accounts.
- Most websites that will be used for IPN offer a minimal amount of free email In the event an email account is shared, anecdotal evidence those accounts tend to belong to partners in an open relationship who are seeking additional sexual partners.

Every possible attempt to confirm that an email has been delivered and read should be made. When using Email clients such as Outlook a delivery receipt and a 'read' receipt may be requested to confirm that an email has been delivered. An email confirming delivery will be

sent automatically, a 'read' receipt requires the receiving party to approve delivery of a 'read' confirmation. For more information on using email confirmation within Outlook review this website:
https://support.office.com/en-us/article/Email-94275804-7147-4332-9ccd-5d421760a9ed#ID0EAABAAA=Compose_or_reply

When sending an email through a website's proprietary email system you may or may not know the status of an email after it has been sent depending on the venue. Websites such as Manhunt will show the status of a sent mail (sent, read, and deleted).
To ensure consistency and to assist in authenticating the legitimacy of PN email, each DIS authorized to conduct IPS will use the appropriate work email address from the agency domain.

Third Party Sites

Third party sites such as InSpot, an e-card notification system (www.inspot.org), have been developed in an attempt to automate partner notification and provide a means for anonymous contact notification.

There is limited data available on the success of third party notification sites such as InSpot. Therefore, it is recommended that more traditional methods such as provider, partner, and contract referrals be the primary referral methods. Third party PN sites should be considered when traditional methods or IPS are not successful or possible.

Joining Online Sites to Conduct IPS

Online sites can be web-based or mobile applications (app) accessed through internet service on the mobile device.

Examples of websites that you may need to use to conduct IPS would be, Manhunt, AdultFriendFinder, BCGLive and potentially many others. Examples of mobile apps that you may need to use to conduct IPS would be Jack'd, Grindr, Adam4Adam Radar, Scruff and potentially many others.

There are many ways sites can be used in conducting IPS. Partner Notification and any follow-up from this process would be the primary use. The effective use of dating/hook-up/social networking websites/apps can also help to find partners, get background information on an OP, and show personal linkages to other potential partners.

Different sites attract different populations and with different populations, the type of IPS performed will vary. For example, a website that is populated with a younger demographic may be used to contact female heterosexual partners who are under 18 and have been exposed to a disease such as Chlamydia, where as a website such as Manhunt that is populated with an older MSM population may be used to contact older male patients exposed to HIV. Specific websites/apps may simply be used to conduct background information on an OP. It is important to realize that language, sexual behaviors, and community norms will vary even within the same community.

When an OP lists a website such as Manhunt, Gay.com, or any other social, membership-based website/app, as the venue of potential disease transmission and the only means of

contact with partners, it will become necessary to join the website/app to conduct partner services. Some websites/apps have policies and procedures for setting up an IPS profile, some do not.

Only DIS that have been thoroughly trained and directed by management specifically to perform IPS are to attempt to join a website/app with the intent of performing partner notification or any other type of partner service. IPN DIS will record all websites/apps joined.

At no time will any employee ever use their personal profile, email account, chat screen name, or instant messaging identity to conduct any IPS related work.

Terms of Service

When joining any website or mobile application you are required to agree to the terms of service (TOS). These service agreements will ultimately define how confidential communication between persons communicating on that specific website will be. All TOS are a legally binding agreement that outlines the site's operating policies.

Frequently Asked Questions

Frequently Asked Questions (FAQ) are provided to answer questions and serve to explain the site and its offerings. As previously mentioned, although some websites/apps have similar features, each website/app is unique. Reading the FAQs of a website will help you become familiar with features the site offers.

Some websites/apps make accommodations for public health, such as providing official IPN profiles (called Partner Notification profiles on Manhunt.net or Health Counselors on Adam4Adam). While Manhunt posts standard pictures for IPN profiles, Adam4Adam does not.

Creating Profiles

When it has been deemed necessary to join an online community to conduct IPS, the employee will be required to create a profile (such as found on Manhunt).

Profiles and web pages are generally geared towards individuals, not agencies looking to perform IPS; therefore, careful attention to each request for information should be taken. All Internet-based communication that comes from an agency must clearly identify the agency in every possible way. This includes profile or webpage text, images, and other publically available information.

All profiles or pages created that require 'personal' information will clearly identify the agency, not the individual employee. Screen names are your online name and must clearly identify your program. An example of a suitable screen name would be "(insert name of region)HealthDept." The Headline of a profile must identify the agency. The profile text must clearly state that the sole purpose of the profile is to contact potential partners.

The email address that has been assigned from the agency for the purpose of IPS must be used as the email address for registration to any site where IPS is going to be conducted.

All passwords created should be secure passwords, meaning that the password is created using a combination of numbers, characters, at least one capital character, and at least one

special character (such as *&^%$#@). Passwords should be recorded either electronically or on paper, kept in a secure location at all times, or only utilized for IPN.

All images used for IPS pages or profiles will consist of agency logos, or images provided by the website (such as the standard health logo for IPS profiles on Manhunt). **Images of individuals should never be used for IPS**.

Many websites/apps require detailed information such as interests, and activities that an individual may be 'into'. When fields (such as 'things I am into') are required, options that display the healthiest choices available, such as 'safe only' and 'no-pnp' should be selected.

Most profiles require a headline and profile text. A profile headline is analogous to a newspaper headline, it is written as a means of getting quick attention and providing the substance of the article. The profile text is similar to the article, providing details about the subject, with the subject being the member.

The intention of IPS is clear and so must be the headline and profile text. An appropriate headline for TDH would be: *Tennessee Department of Health*. Appropriate profile text would be:

> *If you have received an email from this account, it is because someone you had sex with requested our help notifying you that they have a laboratory confirmed infection. Please read the email I sent you for further information. If you would like to confirm that this is a real profile, please call the Manhunt Health Liaison at 866-424-9999 ext. 8945. If using Adam4Adam include: "If you would like to confirm that this email is real though Adam4Adam please contact support@adam4adam.com*

The following steps will guide you through the process of creating a profile:

1. Read carefully and understand the site's Terms of Service (TOS) and Privacy Policy
2. IPS employees must clearly identify that they represent the Tennessee Department of Health.
3. Never use false personal information unless you are in a situation where the site only allows you to state that you are male when you are female, or a similar circumstance.
4. When an email address is required you must use your work email address i.e., Jdoe@tn.gov
5. Create a headline that clearly states where you are located such as: DavidsonCo.Hlth.Dept. (or spell it out)
6. The screen name you create for your profile:
    a) Will be consistent with your location and appropriate for your purpose (i.e., DavidsonCo.Hlth.Dept.)
    b) Will require your supervisor's approval
7. Passwords:
    a) Documented in a secure location
    b) Unique to IPN

8. Use the TDH logo as an image whenever possible. Beware that some sites may refuse this image; you should always carefully review the TOS and site rules for any possible reference to images posted by health employees.
9. Personal info, interests, and other information regarding likes and dislikes must be chosen based on the options that are the "healthiest" or select "ask me" or leave them blank when possible.
10. Text example: "I work for the (region or county name) department of health as a disease intervention specialist. If you receive a message from this account, it is because someone has requested our help in notifying you about possible exposure to an infection. It is very important to respond to this message."
11. Learn about and understand site/app features such as:
    a) Direct instant message and chat capabilities
    b) The site's email system: is it an open system or a closed system?
    c) Identify features that may make your profile "invisible"
    d) Identify features that may track your movements such as "tracks" or "Who I have viewed" feature
    e) Identify other features such as "block", "buddy" and "favorites"
    f) Learn and practice searching using the different search options on the site
    g) Look for and review any health information that the site may offer
12. Keep a "regular presence" on the sites of which you are a member
    a) Site members may e-mail you with questions because they notice that you work for TDH
    b) Many sites change and update features regularly, always read about and learn new features as thoroughly as possible
    c) Some sites will update features that may require that you "upgrade" or "update" your software to use these new features

Email Format

The following email protocol applies to both internal (proprietary systems) and external email accounts such as Gmail, Hotmail, Comcast, Verizon, etc.

1. The employee will begin by sending a series of emails (see Appendix D) starting with Email #1. If there is no response within 3 business days, then send Email #2.
2. If you do not receive a telephone response from Email #2 within 2-3 additional business days, Email #2 will be re-sent. Only 3 unsolicited emails shall be sent per disease exposure.
3. If the partner requests no further contact, Email "Negative Response" should be sent.

4. If a partner expresses interest in learning more via email and you have exhausted all efforts to engage the partner through traditional means, then the Email "Positive Response" shall be sent.
5. If communication takes place on a website that indicates the last time a member logs in, then Emails 2 and 3 should only be sent if the member has logged on since sending Email 1. If it can be determined that emails 1, 2 and/or 3 have been read but there is no response, review the case with your supervisor and discuss a plan of action (e.g., re-interview the index case to collect additional locating information on this partner).
6. After approximately two weeks (10 business days) from the initial email contact, all notification follow-up activities will be closed (unless the partner initiates further contact) at the discretion of the supervisor.

Every precaution must be taken to ensure that the appropriate partner is notified. Because many screen names are similar, the employee should make every effort to confirm that their email/screen name exists and that the spelling is correct. This can be done on most websites using their search feature and by having the OP physically write the screen name on paper. If identifying information was collected from the OP at the time of the interview, confirm the description with the partner's profile which may include pictures. If the email address or screen name does not exist, the employee must inquire further with the OP regarding the error. Screen names may be very similar and sound the same, for example: a member with the screen name 'partyboi' would be a different user than a member with the screen name 'partyboy'.

At no time will the employee include any information that may identify the index patient or the OP. It is best that a employee err on the side of caution rather than risk releasing any identifiable information to another person.

To encourage patients to read email and avoid appearing as 'spam,' the subject field will be left blank, containing no text.

Screen names should be avoided in the greeting of all emails (Hello screen name). When a conversation has begun using a screen name it is often difficult to move from the use of a screen name into the use of a 'real' name. Real names should be used whenever possible.

Miscellaneous Email Communications

Some communication will require specifically addressing questions or comments that are not covered by the above scenarios. In these situations the comments or questions should be addressed within as much of the framework of the scripts as possible (see Appendix H).

If the contact asks a random question refer them to the most appropriate source of information that can provide additional health materials. A link to a web site such as http://www.cdc.gov/STI would be appropriate for most STI related questions. A link to http://www.cdc.gov/hiv would be appropriate for most HIV/AIDS related questions. Having a referral list for services that offer support regarding mental health or addiction would be beneficial and will provide options for referrals.

Chat and Instant Messaging (IM)

It is possible that the only means of making contact with a partner is through a group or instant messaging a client through a website. Websites and apps such as Facebook and Instagram have the capability to contain both groups and instant messaging. Using a group or instant messaging to contact a partner should be a last resort as groups and IM are less secure and more difficult to document than email.

What is a group?

A group is a page within a website for group communication and for people to share their common interests and express their opinion. They let people come together around a common cause, issue or activity to organize, express objectives, discuss issues, post photos, and share related content. Groups usually require an administrator that will approve or deny someone acceptance to the group. Groups call also be closed or opened. An open group means that anyone can join without approval by the administrator. A closed group means that approval is required. Groups can also be public or secret. A public group means that it can be found within a website by doing a search based off of name or possible interest. Secret groups cannot be found by search and you must be invited in by a current member.

Instant messaging, often shortened to simply "IM", is the exchange of text messages through a software application. Most exchanges are text-only; though popular services, such as KIK, Snapchat, Marco Polo and Apple's iChat now allow other feature such as voice messaging, file sharing, and video chat, when both users have webcams.

For IM-ing to function both users do not have to be online at the same time. If the user isn't online they can receive the message once they log in. Often times they will receive a notification via email that they have a message waiting. If the users are not friends they can either accept or reject the message.

Common software applications for chat such as KIK, Snapchat, Marco Polo and Apple's iChat can only be installed on telephones. The telephone used should be an approved telephone that is only used the IPS DIS. The downloading of these applications on personal telephones to conduct IPS is prohibited.

There are several factors that you should always keep in mind when initiating contact with clients through a group or instant messaging. The person you will be contacting could be engaged in several conversations at once or they may be listed as being 'online.' However, the person may in actuality be logged in, but away from their computer or telephone. Do not expect an immediate response. If there is too much lag time after sending a message, you could continue to try and engage the person by asking "Is this a good time to chat?" or "If you are busy, we can talk later". Under no circumstances should you take an aggressive or 'pushy' approach.

Making Contact in a group

1. Staff will log onto the specific website and do a search for the group. If the group is a closed group staff should send a request the administrator to the join the group.
2. If acceptance is granted staff should review the member list in an attempt to locate the partner. It is important to initiate a private (direct) message with the person you're trying to reach. **Do not** post any comments or text in the public area of the group. Using a "private" message option will ensure privacy. The procedures for conducting a private message will vary by site. In most groups a private message can be started by clicking on the screen name of the person you are trying to reach and identifying the chat feature on their profile.

Once you have found the partner online, a sequence of sample messages has been created. This sequence should be followed as closely as possible (Appendix E).

Partner Notification through Text Messaging (txtPN)

Text messaging should be an option for communicating with clients and conducting PN. The goal of text messaging by DIS is to motivate the recipient to communicate via voice. Conducting PN through text is particularly applicable in situations where a client or partner is not responding to traditional means of follow-up (e.g. phone calls and field visits).

Studies have shown that clients and their partners prefer test messaging as the method of contact, and in some cases, the only means of contact. Text messaging has also been used as the preferred means of communication when a client was hearing impaired. Using text messaging when a patient or partner has a hearing impairment should be presented as an option when possible.

What is Text Messaging?

The terms Short Message Service (SMS) and Text Messaging can be used interchangeably, although SMS is a term more often used within the mobile industry. A single text message can be up to 160 characters in length and can be comprised of words, numbers, or an alphanumeric combination. Some text messages can be longer but will be received in multiple messages.

Currently, text messages can be sent to a mobile phone or communication device in one of three ways: mobile to mobile, internet to mobile, or email to mobile. Be aware that most services that offer free 'web-to-text' or 'internet to mobile' services will include advertisements within the text message that is sent.

How to Access Text Services

Most cell phone carriers will offer their own web-to-text service. When the carrier is known (obtained through a reverse search or other methods) the web-to-text tools provided by the carrier may be used as an alternative to using a cell phone when a cell phone is not available or when a texting plan is not available. (Examples of web-to-text tools include: https://text.vzw.com) When the carrier information is incorrect it is most likely that the message sent though the carrier's site will not be delivered.

DIS are to make every effort to confirm that the contact number given is associated with a cellular phone and who the current carrier is. Using a third party service, such as a free web-to-text service found on the internet, may not be a secure method of communication and could expose the DIS, their clients, and patients to spyware, cell phone spam, and possibly have other undesired outcomes; therefore , DIS are not to utilize free, third party web-to-text sites to contact clients or partners.

How to Conduct txtPN

A text message should be sent in order to prompt the person to respond. Some carriers will provide you with an option to receive a text message delivery confirmation. This service, where available, is requested by you through the settings on your cellular phone or through your carrier account preferences.

Most of the major carriers including but not limited to: Sprint, Verizon, and T-Mobile, offer a service called 'Text to Landline" (https://www.verizonwireless.com/support/text-to-landline-faqs/). Text to Landline will allow you to send a text messages from your cellular phone to a 'land line' automatically converting the text to a computerized voice call. This is of particular importance when it is assumed that the contact number that has been provided is a cellular number but the number is actually associated with a 'land line'.

When conducting txtPN, messages must be sent from a work phone or a work computer. Personal cell phones or computers should not be used to communicate with clients or their partner(s).

Sending a text message carries similar confidentiality risks to leaving a voice mail message on an answering service. DIS should remember that text messages can be viewed by people other than the intended recipient if they have access to the mobile phone of the person receiving the text message. Broad language is to be used when communicating via text message. Disease specific information is not to be exchanged through text messaging.

As cell phones are wireless devices and can be used anywhere. Text messages must be sent when DIS are in a space that offers privacy. Should the recipient respond quickly; the DIS must be prepared to respond quickly, communicate confidentially, and have access to any resources that may be needed to conduct partner services. Never send a text message while driving or otherwise preoccupied.

Receiving Responses

Text messaging is a rapid means of communication. When DIS are contacted through text message a timely response will be anticipated by the sender. When a DIS receives a reply to a text message, responding in a timely manner will help ensure success and is similar to the importance of quickly building rapport during an original interview.

DIS will begin by sending a series of text messages (Appendix F). As with internet partner services, when sending a text message send one message to one phone at a time, do not send multiple messages to multiple phones, and do not forward messages.

If the DIS receives confirmation that the first text message has been delivered and has not received a response within 3-6 hours, the DIS will send a second text message, at another time of day. It is important to remember that text messages can be received at any time of day

or night and you should be aware that you may receive a reply to your text message at any time of day or night.

If you have not received a reply to the second message, the DIS will send a final message within 6-12 hours.

Text messages that are received should be responded to with a text message unless a voice call has been agreed upon. Once contact has been established, the next text message from the DIS should be a request that the conversation be further conducted though a 'voice call'. If DIS are already communicating with a client or patient in others ways, such as through email, and believe that a text message may be a more effective, be sure to ask the client if texting is acceptable before sending any messages.

Similar to other partner services logs, cell phones used for communicating with clients or their partners contain a history of communication and must be secured at all times and locked with the screen turned off or darkened when not in use. Phone numbers and messages exchanged with clients or their partners must be properly documented in PRISM and deleted from all electronic devices once the case is closed.

The texting history of the case on the mobile device should be cleared and texting should cease once a case is closed.

Documentation

All printed material, such as emails or any other printable correspondence, should accompany the field record and be maintained in a secure location.

Case Follow-up and Contact Tracing

IPS Patient Follow-up

When a partner calls or arrives at a clinic, they must be asked how they were notified of their possible exposure. If the partner was notified through the internet it is likely that there is no record of their real name and the employee should ask about screen names and email addresses for confirmation. The employee should, if available, search the appropriate database to confirm the identity of the partner and update all records. If the employee does not have access to PRISM, the employee should then gather all identifying information possible and search the expected inbox or local logs and records to confirm identity and update the record.

Some individuals will seek services from private medical providers. When possible, the employee should offer to contact the provider (or use Appendix G) on the patient's behalf to expedite their care.

IPS Evaluation

As with traditional partner services, IPS quality assurance and monitoring must be conducted through frequent, routine, and standardized evaluation.

Agencies that are authorized to conduct IPS must have mechanisms in place that ensure that

the program is meeting its goals and objectives and that all related program policies and procedures are being followed. Evaluation, documentation, and quality assurance measures are critical to the success of any disease intervention initiative.

Programs must assess and evaluate their efforts on the internet, not only to quantify successes, but to avoid any potentially harmful/unintended consequences.

Out of Jurisdiction (OOJ) Considerations

Geographic and jurisdictional boundaries are not recognized by the internet. Patients and their partners frequently cross jurisdictions. HIV/STI programs must work together to develop standard protocols for addressing OOJ partners. DIS must work cooperatively with other jurisdictions and agencies to ensure that all partners are informed of possible exposure and that all forms of documentation and tracking are completed as prescribed.

Summary

Internet-based Partner Services provides a means to contact individuals that may otherwise be unreachable, but as experience grows and as technology evolves IPS has the potential to become the preferred method of partner notification and follow-up services. To ensure that partner notification is effective in its mission to reduce STI and HIV transmission, we must utilize new technologies as they are adopted by the general public.

These guidelines outline the tools needed to develop effective IPS activities, and have been created from program experience throughout Tennessee and the nation. The current national STI and HIV program guidelines shared principles for the provision of STI partner services and HIV counseling and referral services remain in effect and applicable when using the internet for partner services.

STATE OF TENNESSEE

Acceptable Use Policy
Network Access Rights and Obligations

Purpose:
To establish guidelines for State-owned hardware and software, computer network access and usage, Internet and email usage, telephony, and security and privacy for users of the State of Tennessee Wide Area Network.

Reference:
Tennessee Code Annotated, Section 4-3-5501, et seq., effective May 10, 1994.
Tennessee Code Annotated, Section 10-7-512, effective July 1, 2000.
Tennessee Code Annotated, Section 10-7-504, effective July 1, 2001.
State of Tennessee Security Policies.

Objectives:
- Ensure the protection of proprietary, personal, privileged, or otherwise sensitive data and resources that may be processed in any manner by the State, or any agent for the State.
- Provide uninterrupted network resources to users.
- Ensure proper usage of networked information, programs and facilities offered by the State of Tennessee networks.
- Maintain security of and access to networked data and resources on an authorized basis.
- Secure email from unauthorized access.
- Protect the confidentiality and integrity of files and programs from unauthorized users.
- Inform users there is no expectation of privacy in their use of State-owned hardware, software, or computer network access and usage.
- Provide Internet and email access to the users of the State of Tennessee networks.

Scope:
This Acceptable Use Policy applies to all individuals who have been provided access rights to the State of Tennessee networks, State provided email, and/or Internet via agency issued network or system User ID's. The scope does not include State phone systems, fax machines, copiers, State issued cell phones or pagers unless those services are delivered over the State's IP network.

Use and Prohibitions:

A. Data and Information Technology Resources

State employees, vendors/business partners/subrecipients, local governments, and other governmental agencies may be authorized to access state data or Information Technology (IT) network resources to perform business functions with or on behalf of the State. Users must be acting within the scope of their employment or contractual relationship with the State and must agree to abide by the terms of this agreement as evidenced by his/her signature. It is recognized that there may be incidental personal use of State IT Resources. This practice is not encouraged and employees should be aware that all usage may be monitored and that there is no right to privacy. Various transactions resulting from network usage are the property of the state and are thus subject to open records laws.

Prohibitions

- Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation.
- Installing software that has not been authorized by the Office for Information Resources of the Department of Finance and Administration.
- Attaching processing devices that have not been authorized by the Office for Information Resources of the Department of Finance and Administration.
- Using data and IT resources to play or download games, music or videos that are not in support of business functions.
- Leaving workstation unattended without engaging password protection for the keyboard or workstation.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using data and IT resources in support of unlawful activities as defined by federal, state, and local law.
- Utilizing data and IT resources for activities that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.

B. Email

Email and calendar functions are provided to expedite and improve communications among network users.

Prohibitions

- Sending unsolicited junk email or chain letters (e.g. "spam") to any users of the network.
- Sending any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs.
- Sending copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher.
- Sending or receiving communications that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.
- Sending confidential material to an unauthorized recipient, or sending confidential e-mail without the proper security standards (including encryption if necessary)

being met.

Email created, sent or received in conjunction with the transaction of official business are public records in accordance with T.C.A 10-7-301 through 10-7-308, and the rules of the Public Records Commission. A public record is defined as follows:

> *"Public record(s)" or "state record(s)" means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. (T.C.A. 10-7-301 (6)).*

State records are open to public inspection unless they are protected by State or Federal law, rule, or regulation. Because a court could interpret state records to include draft letters, working drafts of reports, and what are intended to be casual comments, be aware that anything sent as electronic mail could be made available to the public.

C. Internet Access

Internet access is provided to network users to assist them in performing the duties and responsibilities associated with their positions.

Prohibitions

- Using the Internet to access non-State provided web email services.
- Using Instant Messaging or Internet Relay Chat (IRC).
- Using the Internet for broadcast audio for non-business use.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using the Internet when it violates any federal, state or local law.

Statement of Consequences

Noncompliance with this policy may constitute a legal risk to the State of Tennessee, an organizational risk to the State of Tennessee in terms of potential harm to employees or citizen security, or a security risk to the State of Tennessee's Network Operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the State network could lead to liability on the part of the State as well as the individuals responsible for obtaining it.

Statement of Enforcement

Noncompliance with this policy may result in the following immediate actions.

1. Written notification will be sent to the Agency Head and to designated points of contact in the User Agency's Human Resources and Information Technology Resource Offices to identify the user and the nature of the noncompliance as "cause". In the case of a vendor, subrecipient, or contractor, the contract administrator will be notified.
2. User access may be terminated immediately by the Systems Administrator, and the user may be subject to subsequent review and action as determined by the agency, department, board, or commission leadership, or contract administrator.

STATE OF TENNESSEE

Acceptable Use Policy
Network Access Rights and Obligations
User Agreement Acknowledgement

As a user of State of Tennessee data and resources, I agree to abide by the Acceptable Use Network Access Rights and Obligations Policy and the following promises and guidelines as they relate to the policy established:

1. I will protect State confidential data, facilities and systems against unauthorized disclosure and/or use.
2. I will maintain all computer access codes in the strictest of confidence; immediately change them if I suspect their secrecy has been compromised, and will report activity that is contrary to the provisions of this agreement to my supervisor or a State-authorized Security Administrator.
3. I will be accountable for all transactions performed using my computer access codes.
4. I will not disclose any confidential information other than to persons authorized to access such information as identified by my section supervisor.
5. I agree to report to the Office for Information Resources (OIR) any suspicious network activity or security breach.

Privacy Expectations

The State of Tennessee actively monitors network services and resources, including, but not limited to, real time monitoring. Users should have no expectation of privacy. These communications are considered to be State property and may be examined by management for any reason including, but not limited to, security and/or employee conduct.

I acknowledge that I must adhere to this policy as a condition for receiving access to State of Tennessee data and resources.

I understand the willful violation or disregard of any of these guidelines, statute or policies may result in my loss of access and disciplinary action, up to and including termination of my employment, termination of my business relationship with the State of Tennessee, and any other appropriate legal action, including possible prosecution under the provisions of the Computer Crimes Act as cited at TCA 39-14-601 et seq., and other applicable laws.

I have read and agree to comply with the policy set forth herein.

Type or Print Name	Last 4 digits of Social Security Number
Signature	Date

Appendix B - *Employee Confidentiality Statement*

State of Tennessee
Department of Health

Computer Access Security Agreement

I hereby acknowledge receipt of my computer access code(s) and my use of them demonstrates my agreement to the following guidelines:

1) I shall maintain confidentially all computer information and resources to which I have access or control.
2) I shall take appropriate measures to safeguard and protect the information and computer resources of the State that are available to me.
3) I shall use the information and computer resources only for authorized State business and not disclose any information or documentation obtained from, or pertaining to, the State's computer system(s) to any third party, except in the routine lawful conduct of the State's business.
4) I shall be accountable for and accept full responsibility for all transactions performed using my computer access codes.
5) I shall maintain all computer access codes in the strictest of confidence; immediately change them if I suspect that their secrecy has been compromised and report suspected misuse to the respective Security Administrator.

I have read and agree to comply with the guidelines set forth above.

I understand that willful violation of, or disregard for, any of these guidelines may result in disciplinary action up to and including termination of my employment, termination of my business relationship with the State of Tennessee and possible prosecution under the provisions of the Computer Crimes Act as cited at *TCA 39-14-601 et seq.*

_____	_____
Type or Print Name	Social Security Number
_____	_____
Signature	Date
_____	_____
Due to be returned to Sec. Admin.	User ID

Appendix C - Internet -based Partner Services Interview Format

1. What sites are you a member of?
2. What is your screen name?
3. What is your email address?
4. When was the last time you had sex with someone you met online?
    a. Which website or telephone application did you meet him/her on? (using open-ended questions)
    b. Where did you physically meet to have sex? (What was the address?)
    c. What was his/her name?
    d. What is his/her email address?
    e. What is his/her screen name?
    f. When is a good time of day or a certain day that would be best to find this person?
    g. What can you tell me a little about him/her? What does he/she looks like? How is he/she built? What does his/her online profile look like?
    h. What other websites have you seen him/her on? What were his/her screen names?
    i. What is his/her phone number?
    j. What other ways do you contact him/her?
    k. What is your screen name on this website/telephone application?
    l. What time of day do you log on? How often?
5. Before this person, when was the last time you met someone from online?
6. Tell me about your "Friends List" on (Facebook, SnapChat, Adam4Adam, etc)?

Notes:
• Try to get the patient to write down the contact information in order to ensure you have the exact spelling of the screen names.

• Some websites allow you to access profiles without being a member. For example, Manhunt will allow a personal URL to access a profile; the format it http://my.Manhunt.net/(screen name). The format for gay.com is the same (http://my.gay.com/(screen name)

Appendix D - Sample Emails for IPN

Partner Notification Email 1

To: <screen name/email address>
From: Name@tn.gov
Subject: (leave blank)

Hello <name, if known>, (do not use screen name)

My name is _____ and I work for the Tennessee Department of Health. I am contacting you because someone who was recently diagnosed with a laboratory confirmed infection asked that you be notified of an exposure to this infection.

It is important that you call me at _____ so I can speak with you confidentially about the specific exposure and provide you with options for testing and treatment.

To confirm this email is authentic and legitimate, you can call my supervisor _____ at ###-###-####.

Thank you for your prompt response.

DIS name
DIS title
Phone #
Email address

CONFIDENTIALITY STATEMENT: *This letter may contain confidential information belonging to the sender. If you are not the intended recipient or agent responsible for delivering this document to the intended recipient, you are hereby requested to immediately notify us. Any disclosure, copying, distribution or taking of any action about this letter is strictly prohibited by law.*

All emails must contain the above Confidentiality Statement

Partner Notification Email 2

To: <screen name/email address>
From: Name@tn.gov
Subject: (leave blank)

Hello <name, if known>, (do not use screen name)

A few days ago, I sent you an email, but I have not heard back from you.

My name is _____ and I work for the Tennessee Department of Health. I am contacting you because someone who was recently diagnosed with a laboratory confirmed STI asked that you be notified of an exposure to this infection.

It is important that you call me at _____ so I can speak with you confidentially about the specific exposure and provide you with options for testing and treatment.

To confirm this email is authentic and legitimate, you can call my supervisor _____ at ###-###-####.

Thank you for your prompt response.

DIS name
DIS title
Phone #
Email address

Partner Notification Email: Negative Response or No Response

To: <screen name/email address>
From: Name@tn.gov
Subject: (leave blank)

Hello <name, if known>, (do not use screen name)

Thank you for your response.

If you change your mind and would like to learn more about your exposure to a sexually transmitted infection (STI), you may call me and I can tell you more.

In addition, you may print this email and take it to your doctor/hospital/clinic or to the local health department and the medical provider can contact me.

I urge you to please seek immediate medical evaluation. You may also require treatment. STI evaluation and treatment would be free of charge for you at your local health department.

It is important that you understand that many STIs, including HIV, are asymptomatic, which means you can be infected but not show any visible signs of infection. If an infection is not treated, some STIs may cause serious long-term complications.

If you were recently tested for STIs and HIV, I still encourage you to be tested again as soon as possible. This is because some STIs take time to develop in the body before the screening tests become positive. Even if you test negative, some STIs can be prevented if you receive medication.

If you have any further questions now or in the future about the infection to which you have been exposed or the treatment you may have received, please contact me.

This is the last email you will receive from me regarding this STI exposure unless you respond.

Thank you,

DIS name
DIS title
Phone #
Email address

Partner Notification Email: Positive Response

To: <screen name/email address>
From: Name@tn.gov
Subject: (leave blank)

Hello <name, if known>, (do not use screen name)

I wrote you because someone who was recently diagnosed with a laboratory confirmed sexually transmitted infection STI asked that you be notified of your exposure to this infection.

According to the Centers for Disease Control and Prevention (CDC) guidelines, you need to be tested immediately for this infection. You may also need to be treated either because you have the infection or to prevent you from getting the infection from this exposure.

To find out more about this infection:

1. You can call me at ###-###-#### and I can tell you more including where to be tested and treated for free. All of our communications are strictly confidential.
2. Print this email and take it to your doctor/hospital/clinic or to your local health department's free specialty clinic and the medical provider can contact me.
3. Go to http://www.cdc.gov/STI/default.htm to read more about the disease.

I urge you to seek immediate medical evaluation.

It is important that you understand that many STIs, including HIV, are asymptomatic, which means you can be infected but not show any visible signs of infection. If an infection is not treated, some STIs may cause serious long-term complications. We recommend that you test for all common STIs and HIV.

If you were recently tested for SIs and HIV, I still encourage you to be tested again as soon as possible. This is because some STIs take time to develop in the body before the screening tests become positive. Even if you test negative, some STIs can be prevented if you receive medication.

If you have any further questions now or in the future about the infection to which you have been exposed or the treatment you may have received, please contact me.

DIS name, DIS title
Phone #
Email address

If the Contact States "I don't have any symptoms." or "I was just tested."

To: <screen name/email address>
From: Name@tn.gov
Subject: (leave blank)

Dear <name, if known>, (do not use screen name)

I wrote you because someone who was recently diagnosed with a laboratory confirmed sexually transmitted infection STI asked that you be notified of your exposure to this infection.

It is important that you understand that many STIs, including HIV, are asymptomatic, which means you can be infected but not show any visible signs of infection. If an infection is not treated, some STIs may cause serious long-term complications. We recommend that you test for all common STIs and HIV.

If you were recently tested for STIs and HIV, I still encourage you to be tested again as soon as possible. This is because some STIs take time to develop in the body before the screening tests become positive. Even if you test negative, some STIs can be prevented if you receive medication.

It is important that you call me at ###-###-#### so I can speak with you confidentially about the specific exposure and provide you with options for testing and treatment.

In addition, you may print this email and take it to your doctor/hospital/clinic or to your local health department and the medical provider can contact me.

Thank you,

DIS name
DIS title
Phone #
Email address

If the Contact States "Thank you for the information. I will check with my doctor."

To: <screen name/email address>
From: Name@tn.gov
Subject: (leave blank)

Dear <name, if known>, (do not use screen name)
I am glad to hear you will see you medical provider. If you or your doctor would like to know more about the specific infection to which you have been exposed, please contact me.
According to the Centers for Disease Control and Prevention (CDC) guidelines, you need to be tested immediately for this infection. You may also need to be treated either because you have the infection or to prevent you from getting the infection from this exposure.
I will follow up with you next week to see how your doctor's visit went.

Thank you,

DIS name
DIS title
Phone #
Email address

If the Contact States "This is a hoax."

To: <screen name/email address>
From: Name@tn.gov
Subject: (leave blank)

Dear <name, if known>, (do not use screen name)

This is not a hoax or spam mail. I am not trying to deceive you.
My name is _____ and I work for the Tennessee Department of Health. I am contacting you because someone who was recently diagnosed with a laboratory confirmed sexually transmitted infection asked that you be notified of an exposure to this infection.

It is important that you call me at ###-###-#### so I can speak with you confidentially about the specific exposure and provide you with options for testing and treatment.

If you do not want to continue to communicate with me, you may print this email and take it to your doctor/hospital/clinic or to your local health department and the medical provider can contact me.

I can help you get tested for free today.

Thank you,

DIS name
DIS title
Phone #
Email address

Appendix E - Sample Chat Messages

First Attempt

Hi, this is <___> from <___> my phone number is <Insert specific employee/agency telephone number that handles PN calls>. Is this a good time to talk?

If response is "yes": ask "Are you the only person who uses this screen name?"

If "yes" state,

I need to speak with you about an important health matter. In order to protect your privacy and because we are not communicating on a secure site, it is important that you call me-- (ask for (insert employee name)) at (Insert specific employee/agency telephone number that handles PN calls). Or, if you prefer, I can call you.

If the client responds "no" (or other inconclusive or negative response) ask: "Is there a better time to talk to you"?

If yes—find out when and say "I'll try again then" and end the attempt

If "no response" to your initial attempts, ask "Are you there". If still no response—keep the IM open until the client responds or too much time has elapsed—generally one hour or greater (then try again another day).

If no response, 2-3 days later, try again

Second Attempt

This is <___> again from <___>. I tried to talk to you last <fill in day you last tried>. What I need to discuss with you is a serious health issue. Please call me at <Insert specific employee/agency telephone number that handles PN calls>. Or, I can call you directly if you provide a number and time where I can reach you.

If no response, try again 2-3 days later

Third Attempt

This is <___> again from the (fill in agency name). I've tried to contact you on two other occasions. What I want to discuss with you is a serious health issue. It is urgent that you contact me (or provide a number and time where I can reach you). Please call me at (Insert specific employee/agency telephone number that handles PN calls).If I don't hear from you, there will be no further attempts from me to contact you.

Appendix F - Sample Text Messages/ Instant Messages

Your first text message/ instant message should identify who you are and/or where you work and provide a brief message and your contact phone number.

First Attempt

I am < > with the (fill in agency name) and I need to speak with you. Please call me as soon as possible at ###-###-####.

I am with the (fill in agency name) and I have important information regarding your personal health, please call as soon as possible ###-###-####

Hi _____, I am with the (fill in agency name) and I have information regarding an urgent health matter, please call ###-###-####.

Second Attempt

If the person does not respond to your initial text within 24 hours a second message urging the person to call you may be sent and it should read:

This is < > again with the (fill in agency name)*).* I need to talk to you regarding an urgent health matter, please call me at ###-###-####.

This is < > again with the (fill in agency name)*).* I have urgent health information for you. Please call me at ##-###-####.

Third Attempt

I have been trying to contact you as it is very important that we talk. Please call me at ###-###-####. This is my last attempt to help you.

More Information Requested

I am not able to give you the specific information in text message/ instant message this is urgent and needs your immediate attention. Please call me at ###-###-####.

This is a serious matter, I can tell you more when you call, please call me through a private line at ###-###-####.

The information I have for you is confidential. I can tell you more when you call, please call me through a private line at ###-###-####.

Appendix G - IPS Log

Internet-based Partner Services Supervisory Website Log

Date	Website/Mobile App	Log In Time	Log Out Time	Purpose	Staff/Sups Initials

Appendix H - Glossary for IPS

404 error - Error returned by a browser when it is unable to connect to a remote address

Adware - Software that serves banner ads or pop-up ads while in use; often installed in freeware or shareware downloaded from the internet and provides a channel for advertisers to reach and potentially track your movements around the internet; some more sophisticated versions of adware may also track files, net usage, and installed software and report it back to advertisers so they can display ads that match your traffic pattern

Applet - A small application that is downloaded from a web page and executed by browser software (also, an HTML tag that defines an applet program)

Application software – commonly known as app(s); software designed to perform a group of coordinated functions, tasks, or activities for the benefit of the user

Avatar - Used mostly in chat rooms, social networking sites, and in games to represent a person, usually the participant; a variant is a profile picture which can also be an actual picture of the user; commonly abbreviated as 'avi'

B2B Business to Business - B2B is the exchange of products, services, or information between businesses conducted over the internet rather than between businesses and consumers.

Backbone - A central network connecting other networks together; formerly a network run by the National Science Foundation, there are now numerous backbones run by commercial providers such as MCI, Sprint, UUNET, and AT&T

Bandwidth - Literally, the frequency width of a transmission channel in Hertz, kilohertz, megahertz, etc.; often used as a way to express the amount of data that can be sent through a circuit; the greater the bandwidth, the greater the amount of data that can travel in a given time period (see also broadband)

BBS - Bulletin Board System; a dial-up service offering messages, files, and other services over a modem; largely replaced by the internet

BCC - Blind Carbon Copy; unlike the cc option (Carbon Copy), when the bcc address option is selected in e-mail, other addressees do not see the bcc address.

Bio – a short introductory message used on websites, social media accounts, dating/hookup apps, blogs, etc.

Blog - Short for web log; usually a chronological record of thoughts, links, events, or actions that are posted on a web site or webpage

Bookmark - Similar to a paper bookmark, electronic bookmarks are used to bring you back to a website you may want to return to in the future by saving the link; a variant is favorite

Broadband – a wide bandwidth data transmission that can simultaneously carry many channels of information; fiber optic cable, in particular, has a very high bandwidth

Browser - Software that interprets the HTML or XML code from the web page files and executes scripts and programs

Cache - Disk memory space that is pieces of recently visited web files, both HTML and binary files, used in an attempt to save time when loading the same webpage again

CC – Carbon copy; used as a merely formal indication of the distribution of emails to secondary recipients

Chat - A form of real-time electronic communications where participants type what they want to say, and it is repeated on the screens of all other participants in the same chat room

Client - An individual computer on a network that runs its own programs and processes information that is received from a central server.

Computer – an electronic device for storing and processing data, typically in binary form, according to instructions given to it in a variable program

Cookie - A short file which includes information about your usage and facilitates interaction with websites; may include the information that you have logged into a password secured area or website and don't need a second password check; may be erased at the end of a session or retained until the next session; most cookies have an expiration date or time, and they may be encrypted or in plain text

Child Online Protection Act (COPA) - The 1998 act of Congress intended to protect minors from exposure to pornography

Children's Online Privacy Protection Act (COPPA) - The act of Congress developed for the protection of children

Copy-and-paste, Cut-and-paste - The technique of copying text from one location or file to another; if the text in the original location is deleted, it is called cut-and-paste; whether cutting or copying, the process begins by positioning the cursor at one end of the text to be copied, and clicking and dragging to the other end to highlight the text or if you want to copy the entire text on a page, use Edit/Select All or press Control and the letter A simultaneously

Copyright - The legal protection against copying and the specific rights allowing copying given to original works, which may be in printed or photographically or electronically stored words, music, visual arts, and performing arts

Country Code - Most countries have been assigned two-letter country codes by the international standard ISO 3166; these two letter codes are the major domain addresses for the country such as .us, or .co.uk

Database - A collection of data records

Direct Message – The function that enables you to send a private message to a person; commonly abbreviated as 'DM'

Disk Operating System (DOS) - The portion of an operating system that controls writing, storage, and retrieval of data from storage media, usually spinning disks of various types; in common usage, the term refers to MS DOS, the operating system developed by Microsoft for IBM-compatible personal computers in text modes

Domain Name System (DNS) - DNS servers are located at many strategic places on the nets to resolve the routing of e-mail and internet connections; there are thirteen major, top-level DNS servers, which are updated daily, and these in turn feed the updated DNS information to smaller subordinate DNS servers, which hold more detailed information on their specific areas of coverage; no single DNS server has all the address information of the internet and successful routing may require routing through several levels of servers.

Domain Name - the name of the website or URL, and is sometimes called the host name; one of two forms of internet addresses in common use together with IP addresses; domain name addresses all end with a correct top-level domain; the top-level domains may be any of these:

- com
- edu
- gov
- int
- mil
- net
- org
- biz
- pro
- museum
- aero
- name
- coop
- info
- a two-letter country code, such as us, uk, or mx.

Dot-com - Nickname for the many commercial businesses that have registered names in the .com domain

Download - To transfer a file from another system to your own computer system

DSL - Acronym for Digital Subscriber Line or Digital Subscriber Loop, often referred to as xDSL; refers to digital technologies for fast two-way data connections over ordinary telephone lines

Dynamic HTML (DHTML) - A more powerful model for HTML that allows absolute control of positioning of elements on a page and more exact control of events

E-mail - Electronic mail; one of the earliest standard internet protocols which enables people with different computers and operating systems to communicate with each other; allows one-to-one or one-to-many mailings; mail is received and held by a mail server within an organization or by an internet service provider until the addressee logs on to collect the mail

Emoji - a small digital image or icon used to express an idea, emotion, etc.

Emoticon - An expression formed with typed characters; these are used in place of real facial expressions, body language, and tone of voice when writing.

Ethernet - a series of standards for **communication** between devices

FAQ - Acronym for Frequently Asked Questions; FAQ files are common questions and answers for a particular subject area

Firewall - Refers to the concept of a security interface or gateway between a closed system or network and the outside internet that blocks or manages communications in and out of the system

Flame - To write angry or insulting words about a person; a variant is troll

Flame War - When two or more people exchange insults in a public messaging

Follower – Term used to describe users who 'follow' your account on social media, websites, etc. because of a shared interest or interests; a variant is friend

Freeware - Software that is offered for free download

Gif - A lossless format (type of data compression) for image files that supports both animated and static images

Going viral – The act of a video, image, or story spreading quickly and widely on the Internet through social media and e-mail

Graphical User Interface (GUI) - Pronounced "gooey"; an operating system interface between the user and the computer based on graphics

Hacker - Originally, a hacker was a term of respect among computer designers, programmers, and engineers for those among them who created truly original and ingenious programs, devices, or sometimes very clever practical jokes; the current popular meaning of the term is to describe those who break into systems, destroy data, steal copyrighted software, and perform other destructive or illegal acts with computers and networks

Handle – Your username or personalized URL created for use on social media, online communities, blogs, etc.; may be known as an '@ name'

Hardware – The physical components of a computer

Header – space reserved on a social media account used for an additional picture that may be related to or an extension of a user's avatar/profile picture or aspect of his/her life

Hit - In search terminology, every listing a search engine returns from a search is called a hit; also used to refer to calls on a web server; many people and most 'hit counters' use the term hit to mean hits on the web page only; when someone quotes figures on hits, be aware that definitions and uses vary, and try to find out what definition was used in producing the figures

Home page - A home page is a web page, often a personal website or page for an individual; on most websites, it is the page which a server will show when no HTML filename is listed, usually with the name index.html, home.html, or default.html or the same names with the shorter extension .htm

HTML - Hyper-Text Markup Language is the coding system used to create WWW pages

HTTP – Hyper-Text Transfer Protocol is the main protocol used on the World Wide Web that enables linking to other web sites; addressing to other web pages begins with "http://" and is followed by the domain name or IP address; HTTPS ('S' for secure) is an extension used for secure communication over a computer network

Hyperlink - A link in a web page that brings you to another location or resource when activated; usually appear as underlined text displayed in contrasting color but they may also appear as a graphic such as a buttons

Hypertext - A form of text which includes visible links to other pages of text or media, accessible by clicking or selecting the links

IMAP - Internet Message Access Protocol is the system used to retrieve mail, where the mail resides on the server instead of the client application

Internet – A network of many networks that interconnect worldwide and use Internet Protocol (IP); an internet (lower case i) describes more than one local network interconnected by bridges or routers

Intranet - A network of networks that interconnect within a single widespread organization and use the Internet Protocol (IP); the sites within an intranet are generally closed and are accessible to organization members only

Internet Protocol (IP) - The method or protocol by which data is sent from one computer to another on the Internet; each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet

Internet Relay Chat (IRC)- An internet protocol that allows people all over the world to meet in conference groups (called channels) and chat with each other by typing

IP address - a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication; one of two forms of internet addresses in common use together with domain name addresses; consist of four numbers between 0 and 255, separated by dots

ISDN - Integrated Services Digital Network; technology that carries data over phone lines at up to 128Kbps usually for dial-up users, but extends to fast broadband communications

ISP - Internet Service Provider; an organization that provides services for accessing, using, or participating in the Internet

Java - A programming language developed by Sun Microsystems based on C++; it is used with web pages to create applets that will run on different platforms; JavaScript A is script language developed by Netscape for writing short programs embedded in a web page

LAN - Local Area Network; computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building

Like – A form of notification used on social media and dating/hookup apps that expresses that a user 'likes', enjoys, or supports a post or profile

Link - An active connection to another web page, location in a web page, file, or other internet resource; selecting the link takes you to the new location or resource

Listserv - One of the earliest types of e-mail discussion lists still in widespread use

Lurk - Listening in to a mailing list, message base, chat room, or newsgroup without participating; can also mean to browse a user's social media or dating/hookup app account without some form of interaction with the user (liking, sharing, direct messaging, etc.)

Luser - A user who is a loser; the result of a dispute at MIT some years ago where computer error messages referred to errors by users' others changed users to losers, and the dispute continued until someone coined the term lusers

MAC address - Media Access Control address, given to a device in a network; consists of a 48-bit hexadecimal number (12 characters); the address is normally assigned to a device when it is manufactured.

Mail bomb - Flood a single e-mail address with a high volume of mail

Malware – Malicious soft**ware**; any software intentionally designed to cause damage to a computer, server, client, or computer network

Meme - an activity, concept, catchphrase, or piece of media that spreads, often as mimicry or for humorous purposes, from person to person via the Internet, social networks, blogs, direct email, or news sources

Mobile app – a computer program or software application designed to be used on a mobile device such as a phone, tablet, or smart watch; commonly used to access social media platforms and for dating/hookup purposes

Mobile device – A computing device such as a laptop, cell phone, tablet, etc. that is small enough to hold and operate in the hand for "on the go" purposes

Modem - Short for modulator/demodulator; used between a computer and a phone line (dial-up), cable line (external modem), or wireless connection (internal modem) to convert the computer's digital signal to an analog signal for the line and vice versa

Network - a collection of computers and other devices connected by communications channels, e.g. by ethernet or wireless networking

Newsgroup - See usenet newsgroups

Notification – A message a user receives on an account that informs him/her of some kind of update such as a like, new friend request, direct message, post to a group, etc.

PDF - Adobe's Portable Document Format; it is often used as a format which allows much more complete, controlled layout of a page and its graphics and text than conventional HTML does

Phishing – The fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication (email, direct instant message, etc.)

Plug-in - A piece of software that plugs into a main program to give it added capability, for example, you can add a Quick Time plug-in to your browser to play Quick Time movies on the web

POP3 - A POP3 (Post Office Protocol) server is used to store email messages; messages are collected from a POP3 (incoming) mail box using an email client such as Thunderbird, Outlook, or Outlook Express.

Post – words, pictures, or videos uploaded to social media accounts, websites, etc.; variants include status (update), tweet, and story

Protocol - A standard created for the exchange of information; computers, operating systems, and software communicate with each other on the internet because of the adoption of protocols

Reverse lookup - A directory service where, given the phone number, address or other information and you can look up the name, phone number, or address of an individual

Router - A device that connects networks together, controlling the 'routing' of packets from source to destination and providing alternate paths when necessary

Server - a system that responds to requests across a computer network worldwide to provide, or help to provide, a network or data service

Share – An offset of a post that allows a user to repost, or 'share', another user's post; variants include retweet (Twitter) and quote (Twitter and message boards)

Shareware - software that is available free of charge and often distributed informally for evaluation, after which a fee may be requested for continued use

Social media - Websites and applications that enable users to create and share content or to participate in social networking (Facebook, Instagram, Snapchat, Twitter, etc.)

Software - A collection of computer programs, libraries, and related data

TCP/IP - Transmission Control Protocol/Internet Protocol; the protocols that are the basis for transmitting and routing data packets on the internet.

Telnet - A protocol that lets you log in to a remote computer and use programs and data that the remote owner has made available

Timeline – A series of posts on a user's social media account that includes both that user and his/her followers posts

TOS - Terms of Service; rules by which one must agree to abide in order to use software or a service; can also be merely a disclaimer, especially regarding the use of websites

Trending topic - A word, phrase, or topic that is mentioned at a greater rate than others and becomes popular either through a concerted effort by users or because of an event that

prompts people to talk about a specific topic; most commonly used on Twitter and denoted by a hashtag

Trojan horse - A destructive program that masquerades as a harmless one; when a Trojan horse program runs it will, for example, erase your hard drive

Upload - To transfer a file from your computer system to another system via a modem over telephone, cable lines, wireless connection, or a telnet connection using a transfer protocol

URL - Uniform Resource Locators specify the location of a resource in the internet; shows the type of item and its basic address and path; major types are http, gopher, ftp, telnet, newsgroups, news articles, and files, which may be programs, text, graphics, audio, video, etc.

Usenet – Also known as newsgroups; usenet newsgroups are discussion groups about a topic that is reflected in their titles, such as comp.sys.ibm.pc.games.adventure or sci.astro.hubble

Virtual Private Network (VPN) - A private network within a public network, usually on the internet; privacy for the virtual network is achieved through encryption and provides a less expensive option than using dedicated lines

Virtual reality - A computer simulation of a real 3-dimensional world, often supplemented by sound effects

Virus - A destructive program that has the ability to reproduce itself and infect other programs, computers, networks, or disks

W3C - Abbreviation for the World Wide Web Consortium, the organization that develops standards for the web community.

WAN - Wide Area Network; a communications **network** that spans a large geographic **area** such as across cities, states, or countries; can be private to connect parts of a business or they can be more public to connect smaller networks together

Web site - One or more connected web pages under a common ownership or management or theme

Wi-Fi - Short for **wi**reless **fi**delity, a standard for wireless ethernet

Worm - A self-replicating program that reproduces itself over a network

WYSIWYG - Acronym for "What You See Is What You Get"; the term applies to word processors and web page development software where you manipulate text and images directly without writing codes (such as HTML or dot codes) for each attribute

XML - Acronym for eXtensible Markup Language is a widely used system for defining data formats; provides a very rich system to define complex documents and data structures such as invoices, molecular data, news feeds, glossaries, inventory descriptions, real estate properties, etc.

Xmodem - An early form of file transmission for dial-up and telnet connections

Zip - a collection of files and/or folders compressed into a single file for easy transportation and compression (identified by a zipper graphic); originally used with MSDOS

Common Email, Chat, and Text Abbreviations

2MOR - tomorrow
ADDY – address
AF – as (expletive)
AFAIK – as far as I know
AMA – ask me anything
BRB - be right back
BTDT - been there, done that
BTW - by the way
FTFY – fixed that for you
FUBAR - Fouled Up Beyond All Recognition (or other less polite forms) by a person giving a commentary on a project or the world in general; often misspelled FOOBAR by people who do not understand its source.
FWIW - for what it's worth
FYI – for your information
<g> -"grin".
GM / GN – good morning / goodnight
HBU – how 'bout you
HMU / HML – hit me up / hit my line (as in call me, text me, etc.)
HRU- How are you
IIRC - if I remember correctly
IKR – I know right
IKYL- I know you're lying
ISO - in search of
LMAO – laughing my (expletive) off
LMK – let me know
LOL - laughing out loud
NVM - nevermind
OFC – of course / of (expletive) course
OMW – on my way
ROFL / ROTFL - rolling on the floor laughing
RTFM - read the fine (or "expletive") manual
SMH – shaking my head
TL;DR – too long; didn't read
TMI - too much information
WYD? – what are you/ 'whatcha' doing?
XOXO – kisses and hugs
YOLO – you only live once

Common Websites/Applications

Adam 4 Adam
Christian Mingle
Daddy hunt
E-Harmony
Facebook

Grindr
Hornet
Jack'd
Manhunt
Match
Plenty of Fish
Scruff
Tindr
Twitter

References

Centers for Disease Control and Prevention. 2015. *Introducing Technology into Partner Services: A Toolkit for Programs. Complete Report*
https://www.cdc.gov/std/program/ips/IPS-Toolkit-12-28-2015.pdf

National Coalition of STD Directors. 20010. National guidelines for Internet-based STD and HIV Prevention: Accessing the power of the internet for public health. Washington, DC National Coalition of STD Directors.

Walsh, C. July 13, 2010. Dear Colleague Letter. Centers for Disease Control & Prevention, July 13, 2010.

Preece, Jenny. 2000. *Online Communities: Designing Usability, Supporting Sociability.* University of Maryland Baltimore County : John Wiley & Sons, 2000.

Ropelato, Jerry. 2008. Internet Pornography Statistics. *TopTenREVIEWS.* [Online] 2008.