Guidelines for Internet-based

Partner Services

Table of Contents

Appendices

1. Introduction

This section of the Internet Guidelines makes recommendations for conducting Internet-based partner services (IPS), which includes Internet-based partner notification (IPN), for both STDs and HIV, in virtual settings, such as through e-mail, instant messaging (IM) and in chat rooms. STD and HIV IPS has been combined into a single set of recommendations, because, while programs may have different approaches to Internet-based STD/HIV work, certain basic programmatic and staff requirements are necessary for the work to be effective. It should also be noted that this document uses the term "partner services (PS)", including IPS, as adopted by the recently revised CDC guidelines for HIV-STD partner services.[1] The term "Partner Services" is broad and encompasses services beyond partner notification (PN); such as STD testing and vaccination recommendations. Moreover, the term acknowledges that persons with STDs often need the same array of services as persons with HIV and that creating distinctions between the two does not serve the best interests of public health or the individuals involved.[1]

The recommendations in this section are based on program experience[2-8], lessons learned from pioneers in the field of IPS, and input from several state health departments and community-based nonprofit organizations. Most of the data driving these guidelines are based on using IPS for infectious syphilis cases. Although these guidelines can easily be modified to include other STDs – such as Chlamydia, gonorrhea, or HIV – and indeed some programs are already using IPS for these infections, the data are not currently available to warrant global guidelines for all STDs.

IPS adheres to the same standards and ethics as traditional PS, and the recommendations presented in this document should be used in conjunction with the CDC's STD Program Operations Guidelines[9] and the CDC's HIV Counseling, Testing, and Referral Guidelines.[10-11] Principles from both documents apply directly to IPS.

For those jurisdictions that plan to implement IPS, these guidelines are intended to assist program managers in developing their IPS activities. For those jurisdictions that have already developed specific policies for IPS, these guidelines are intended to enhance existing practices. Agencies may have internal policies or electronic barriers, such as firewalls, that may impede implementation of Internet-related activities. It is recommended that agencies review state and local laws and health department or agency policies and consult with information technology (IT) departments prior to implementing IPS activities.

2. Background

PS, as traditionally conducted, has been endorsed by the CDC and National Coalition of STD Directors (NCSD) as an effective public health strategy to reduce STD and HIV transmission and associated morbidity. PS attempts to inform people of their potential exposure to STDs, and to refer them into care, thereby breaking the chain of infection and reducing morbidity.

The Internet is a powerful medium for communication and, as such, is a valuable tool for facilitating STD/HIV PS. Research has shown the Internet to be a venue for STD

transmission[12-14] as well as for disease control and health promotion.[15-17] Access to the Internet has become nearly universal for most Americans,[18] and program areas and health departments have been encouraged to incorporate the Internet into their prevention efforts.[19] With the rise of Internet-based social networking, dating, and sex sites, anecdotal evidence suggests that increasing numbers of men who have sex with men (MSM) as well as other high-risk populations are meeting online to arrange anonymous sexual encounters. As a result, individuals who are newly diagnosed with STDs/HIV may know only the screen names and/or e-mail addresses of their sex partners.

The Internet represents a relatively new medium for conducting PS. IPS is the process of using the Internet to conduct or enhance the process of notifying a person of their potential exposure to an infectious disease. IPS should augment traditional methods of PS, specifically provider referral, where appropriate. Partner-locating information is sometimes limited to an e-mail address or screen name/profile on an Internet site, making the use of the Internet the only viable option for providing appropriate STD/HIV partner services in these cases.

Tip from the field

Both the Division of STD Prevention and the Division of HIV Prevention at the U.S. Centers for Disease Control & Prevention encourage the use of the Internet for STD/HIV prevention including IPS.
See the September 13, 2005 Dear Colleague Letter: [19]
http://www.cdc.gov/std/DearColleague9-13-2005.pdf

2.1 Types of Partner Services

Three primary strategies can be used to notify partners of possible exposure to STDs or HIV infection: Provider, Self, or Contact referral. Often, more than one strategy may be used to notify different partners of the same infected patient. The strategy will depend on the particular patient, the particular STD, and partner circumstances. For example, a patient with an STD may feel that he or she is in a better position to notify a main partner, but would prefer that the Disease Intervention Specialist (DIS) notify other partners.[9]

2.2 Principles of Partner Services

Current national STD and HIV program guidelines share core principles for the provision of STD partner services and HIV partner counseling and referral services, and these principles remain applicable when using the Internet for PS. Listed below is the set of principles as described in the newly revised Guidelines for HIV-STD Partner Services.[1]

- **Client-Centered:** All steps of the partner services process should be delivered in a client-centered manner, i.e., tailored to the behaviors, circumstances, and special needs of the person being served.

- **Confidential:** The confidential nature of partner services is essential to its success. This also applies to special protections for data collected as part of the process.

- **Voluntary and non-coercive:** Participating in partner services is voluntary for both the infected person and his or her partners and cannot be conducted in a coercive manner.

- **Free:** There is no charge to infected persons or their partners for partner services.

- **Evidence-based:** Partner services activities should be evidence-based to the extent possible and require knowledge, skill, and training.

- **Culturally, linguistically, and developmentally appropriate:** Partner services are to be delivered in a nonjudgmental manner appropriate to the cultural, linguistic, and developmental characteristics of the person being served.

- **Accessible and available to all:** Partner services must be accessible and available to all infected persons regardless of where they are tested or diagnosed and whether they are tested confidentially or anonymously. Due to the chronic nature of HIV infection, it is also necessary to assure that partner services for HIV are available in an ongoing manner.

- **Comprehensive:** Partner services are part of an array of services that are integrated to the greatest extent possible for persons with HIV or other STDs and their partners.

2.3 Field Experiences

Following are descriptions of experiences from project areas that have developed and implemented IPS programs. These jurisdictions saw an increase in Internet sex partners and adapted their programs to meet the needs of their patients and to address this new venue. Often the only locating information available to the DIS was an e-mail address or screen name. These programs developed procedures and protocols for IPS, learned what worked and what didn't, and paved the way for others. If these sex partners had not been contacted via the Internet, they would not have been notified of their possible exposure to an STD.

San Francisco, California

In 1999, San Francisco conducted a case control study of 7 early syphilis cases that were linked to an online chat room. The mean number of partners per index case was 5.9, and locating information for the sex partners was limited to screen names. Using the Internet to conduct PN resulted in 42% of the named partners being notified and confirmed as having been tested.[2]

In 2003, San Francisco reported that 20.9% of 151 syphilis cases were able to provide only e-mail addresses as locating information for a total of 44 sex partners. Using the Internet, San Francisco Department of Health staff were able to locate 15 (34%) of the Internet sex partners and confirm that they were screened and treated, if necessary.[3] San Francisco had more success reaching those contacts who were first contacted by the original patient (OP) (26/44), with a follow-up by the DIS, as compared to the DIS making first contact.

Los Angeles, California

Two cases from Los Angeles were reported in a 2004 *Morbidity and Mortality Weekly Report* (MMWR) and exemplify how IPS can be an effective, patient-centered approach to PN. In Los Angeles, a high percentage of MSM who were diagnosed with syphilis reported meeting sex partners online. The first case cited an OP who reported 134 male Internet sex partners. He was able to provide the DIS with 111 e-mail addresses and 23 telephone numbers for PN. The Los Angeles County Department of Health Services (LACDHS) sent e-mails to all 111 contacts; 29 persons (26%) responded to the e-mail and were contacted by local DIS.[4]

In the other syphilis case, the LACDHS asked the OP to send an e-mail to his 16 male Internet-sex partners. Of the 16 sex partners, the OP sent e-mails to 13, notifying them of their exposure to syphilis and indicating the health department's desire to refer them to STD clinics for testing and treatment, if necessary. Seven (44%) responded and made arrangements to be tested; suggesting that OP involvement in PN via e-mail may improve partner-response rates.[4] This MMWR also reported that instant messaging (IM) can have similar success for PN.

Philadelphia, Pennsylvania

In 2000, the city of Philadelphia experienced a significant increase in primary and secondary syphilis cases. Through active case management, two infected individuals identified anonymous sex partners met through the Internet chat rooms. These individuals could only provide e-mail addresses for former sex partners. A protocol was developed and implemented to conduct IPS. All DIS, as well as clinical and support staff, were informed of these efforts to insure proper responses to calls generated from IPS. One IPS case resulted in a 60% (3/5) response rate from partners, suspects, and associates. A second investigation resulted in a 40% (2/5) response rate from suspects and associates.[5]

Minnesota

The Minnesota Department of Health also experienced increased cases of syphilis among MSM. Investigation of these cases revealed a cluster of 176 individuals at risk for HIV, syphilis, gonorrhea, and/or Chlamydia infection. In this cluster, 61% (108) of the individuals stated they used the Internet to meet sex

partners. Of these, 50 were locatable only by an e-mail address or screen name. Seven (14%) were out of jurisdiction (OOJ) cases. The remaining individuals were sent e-mails from the health department. Of those contacted, 60% (32) responded to IPS efforts and 26% (13) did not respond at all.[6]

Chicago, Illinois

Howard Brown Health Center (HBHC), a community-based organization (CBO) in Chicago, conducted a comparative analysis of PN initiated via the Internet versus PN via the telephone, the latter being the traditional method of PN. A retrospective case audit was performed for all syphilis cases interviewed by HBHC DIS between January 2005 and September 2006. During that time, there were 304 cases of syphilis followed by HBHC, and these cases produced 368 sex partners. All were included in the overall analysis. IPS was initiated for 190 partners (52%) and telephone PN was initiated for the remaining 178 (48%). Telephone PN was significantly more likely to result in contact between the exposed individual and the DIS. When the analysis was restricted to only those partners contacted regardless of method, there was no significant difference in final disposition (whether or not partners were brought in for testing and treatment, if necessary). Of the 190 sex partners that were contacted through IPS, 30 were found to be infected and brought to treatment and 121 who may not have otherwise had any contact with HBHC, or known of their potential exposure, were provided counseling and referral services.[7]

Boston, Massachusetts

In a national IPS study performed by The Fenway Institute, Fenway Community Health looked at the acceptability of IPS among MSM. A total of 1,848 MSM were recruited online via an Internet sex partner-seeking website between October and November 2005. This study recommended that health departments using IPS use clear and culturally sensitive language when communicating via e-mail. Participants attached a high level of importance in receiving a variety of information in notifications: e-mails informing them that they had sex with someone infected with an STD, linking them to education about the STD, linking them to information on where to get tested for the STD, triage to public health specialists familiar with the STD, as well as access to phone numbers or links to a customer service representative to confirm the e-mail's authenticity. More than 92% of participants reported that they would use IPS in some capacity (i.e., use the department of public health to notify sexual partners using IPS, notify sexual partners themselves via IPS, or do both) to inform their sexual partners if they were to become infected with an STD in the future. The study concluded that IPS should be considered an acceptable tool to decrease rising STD and HIV rates among MSM who use the Internet to meet sex partners.[8]

Based on the above examples, when the only locating information available for a sex partner of an infected individual is an e-mail address or screen name, conducting IPS can

result in partners being notified, then responding to notifications, and, ultimately, being tested and treated for STDs. Additionally, when used after other methods of contact have failed, IPS can increase the chance of eliciting any sort of a response. IPS, therefore,

> **Tip from the field**
> IPS should be viewed as an additional tool for PN and not a separate or different practice.

should be viewed as an additional tool for effective and patient-centered PN, and not a separate or different practice.

3. Before You Begin

3.1 Legal Authority

Before implementing IPS, programs should adhere to applicable state/local laws, regulations, or statutes. A program should assure that policies and procedures developed (e.g., IPS methods, patient confidentiality, ethical conduct of employees) are in compliance with these laws, regulations, and statutes. The HIPAA Privacy Rule allows protected health information to be disclosed by those public health authorities who are mandated to notify individuals of their potential exposure to a communicable disease in an effort to prevent the further spread of disease during the course of a public health investigation. Prior to beginning IPS, programs should review which STDs fall under this rule.[21]

3.2 Confidentiality and Ethics

All PS activities must adhere to standards of confidentiality and ethics. These standards do not change with IPS. Agencies conducting IPS are expected to have a confidentiality policy that specifically covers Internet communication with patients and should include consequences for violations of the policy. These confidentiality agreements should extend beyond staff conducting IPS and includes IT staff and any other staff that may view or have access to confidential information. Such agreements should include statements about the consequence of personal use of health department accounts, e-mail addresses, and health department profiles, as well as statements related to IT access to confidential e-mail or IM. Prior to implementation, agencies need to ensure their HIPAA compliance, use of firewalls, security of wireless networks (if used), and that a policy about permitting staff to conduct IPS from their home computers or laptops is in place. See **Appendix A** for examples of confidentiality agreements.

Screen names, e-mail addresses, HIV status, and/or any personal information are considered to be identifying information and as such are held to the same levels of confidentiality as a patient's first name and surname. Printed documents, such as logs, reports, or transcripts containing screen names or e-mail addresses are to be stored in locked areas. Under no circumstances should staff share any information about IPS

patients with anyone other than affiliated PS staff. E-mail groups and list serves should not be used for PS because patient confidentiality cannot be maintained.

Tip from the field
Amend confidentiality agreements to include e-mail addresses, screen names, and other potentially identifying information.

Staff members need to be trained on IPS policies including what information can be shared and/or discussed over the Internet with infected patients and their sex partners. Some programs require all outgoing e-mails to have a legal disclaimer. See **Appendix B** for an example.

Reasonable efforts should be taken to ensure that e-mails are sent to the intended recipients. The ubiquity of free, password-protected e-mail accounts, screen names, and IM accounts help minimize concerns that erroneous individuals be contacted through IPS. It is important to acknowledge that the potential exists for someone to share an e-mail account or screen name with another person (if they are a couple, for example), but anecdotal evidence from experienced programs have found this not to be the case with the vast majority of e-mail addresses and screen names that are reported to them.

Common concerns about protecting confidentiality

Programs that are new to IPS or newly considering implementing IPS often have concerns about ensuring patient confidentiality and the possibility of breaching confidentiality. The primary concern is that sending an e-mail − especially from an organization that uses the acronym 'STD' in their email address, for example, DCSTD@dc.gov − will unwittingly breach confidentiality if anyone other than the intended recipient of the letter views either the letter or the return e-mail address of the sender. However, few, if any, programs that have been conducting IPS (more than 13 years of combined experience) have experienced these hypothetical scenarios due to the ubiquity of free e-mail accounts, eliminating the necessity of a shared e-mail address. Sending an e-mail carries the same risks as leaving a letter on a doorstep. The same risks exist for both modes of communication, but the public health benefit of notifying someone of their possible exposure and infection outweighs the small possibility that confidentiality will be breached.

Furthermore, descriptive details elicited during the DIS interview with the infected patient (such as race, height, weight, unusual identifying characteristics) should be sufficient to determine that the correct sex partner is being contacted. DIS should also obtain detailed descriptive information about the partner's Internet profile (such as age, height, weight, HIV status, interests, number and type of pictures, and the town and state the profile is listed in) as well as the accuracy of the information listed. If IPS results in the anonymous partner calling the DIS, use of the descriptive information in the profile, along with the information provided by the OP, may be used to verify that the DIS is talking to the correct person. With IPS, the experience reported by many STD programs

is that patient confidentiality can be maintained in the same way that confidentiality is maintained when conducting PN via the telephone.

3.3 Access to the Internet and Computer Security

In order to conduct IPS, employees will need approved access to Internet sites that are traditionally blocked including, but not limited to, social networking, dating, or sexually explicit sites, in addition to the standard resources required as written in the CDC STD Program Operations Guidelines.[9] Access to websites, IM programs, and other communication technologies are essential.

It is critical that IT managers/staff and current program policies and procedures be consulted regarding issues of security, access to sexually explicit websites, etc. prior to implementation of IPS. Potential barriers that may prohibit effective IPS are lack of computer access in clinics, lack of Internet access, lack of computer/Internet knowledge, slow Internet connections, firewalls protecting Internet-enabled computers from gaining access to sexually explicit websites, and local policies restricting the use of the Internet by state and local employees. Procedures securing computer equipment and software used for IPS should be established as well. Anti-virus and anti-spyware software should be kept up-to-date and used at all times on computers used for IPS. Some programs may require a non-networked computer, that is, a computer with Internet access that is separate from the internal network in order to protect servers and to alleviate IT networking concerns. See **Appendix C** for a sample protocol for the use of a stand-alone computer with Internet access.

3.4 Engagement of Appropriate Stakeholders

Engagement of key stakeholders can determine the success or failure of an IPS program. Important stakeholders include, among others, the state Health Commissioner, the Health Department Medical Director, the Health Department Information Technology Director, the Legal Department, persons who will conduct the IPS, STD/HIV Program Managers, DIS, and the at-risk communities themselves. Some stakeholders simply need to be made aware of a program's intention to proceed with IPS; others should be involved in the creation of IPS policies.

Health departments and CBOs conducting PS (hereon referred to as health departments but including all other programs that provide PS) should inform other health department programs, all partnering agencies, community clinics, CBOs, and agencies that service impacted communities that IPS is now offered through the health department. Ongoing communication with these agencies is critical. Often patients will call these agencies to confirm that the attempt to reach them is valid and the verification can expedite the time the patient takes to respond to the e-mail notification.

Health departments should also notify all private health care providers of this new approach to PS. Many individuals may contact their private physician long before making any attempt to contact the health department. Private physicians can help validate IPS as a new activity used by the health department. Given that many STD cases

are diagnosed in private settings, special emphasis on effective collaboration with private providers is crucial and mutually beneficial for health care providers, health departments and patients. Some health departments provide in-service training regarding the health department's IPS work to hospitals, health centers, and private providers to help them understand PS.

4.0 Evaluation of Internet Partner Services (IPS)

As with traditional PS, IPS quality assurance and monitoring must be conducted through frequent, routine, and standardized evaluation. However, IPS is unique in that (1) staff will have the ability to access adult-oriented websites and (2) a written record of all communication between DIS and those they contact will exist. In some program areas, the ability of staff to access sexually explicit websites at work may not be widely understood or recognized as an effective means of conducting disease intervention and may bring unwanted public and/or political fallout. Organizations conducting IPS activities should have mechanisms in place to ensure that the program is meeting its goals and objectives and that all related program policies and procedures are being followed. Evaluation and quality assurance measures are critical to the success of any disease intervention initiative. STD programs should assess and evaluate their efforts on the Internet, not only to quantify successes but to avoid any potentially harmful/unintended consequences.

Logic models are an effective way of clearly outlining the steps and desired outcomes of IPS and may help in developing evaluation protocols. For examples of logic models, see **Appendix D.** The CDC recently released a valuable evaluation manual specific to STD programs, "Practical Use of Program Evaluation among STD Programs".[21] We recommend that STD programs use the manual to guide evaluation efforts including the development of a logic model.

Tip from the field
Obtain a copy of the manual:
Practical Use of Program Evaluation among STD Programs
http://www.cdc.gov/std/Program/pupestd.htm

4.1 Documentation

Documentation is vital to the evaluation of PS, and therefore to IPS as well. Quality assurance activities can include various data collection forms or secure, password-protected databases, including contact and referral logs, activity report forms, and activity observation tools. See **Appendix E** for a sample log.

Agencies may want to consider collecting printed or electronically stored transcripts of IPS activities, including e-mails or IMs sent and/or received, when feasible (some

websites restrict the ability to cut and paste or otherwise save chat room or messaging text, one way to circumvent this barrier is "printscreen", a keyboard option located in the upper right hand corner of PC keyboards, and then "Paste" in a document). Transcripts can be used for qualitative analysis or to determine factors that influence the high-risk behaviors of individuals online. Monitoring this information will inform evaluation efforts, ensure that protocols and guidelines are being followed, and indicate when program modifications are necessary.

Process measures are those activities that are conducted during implementation of a program and include such things as developing program-specific guidelines and providing IPS training to relevant staff. Outcome measures capture the end effect of your efforts and include items such as the number of individuals contacted, number who responded to IPS, number referred to services, number tested, number who test positive for the infection they may have been exposed to, and/or number of individuals treated. These measures should be captured by staff on interview record forms.

Below is a list of some of the ways in which IPS programs can be evaluated for quality assurance and effectiveness.

- Require consistent and accurate data collection
- Develop an evaluation and quality assurance process for compiling and analyzing data and for documenting and reviewing outcomes
- Provide IPS staff with evaluations and feedback
- Develop a means for patients to provide feedback
- Define methods for assessing progress toward stated process goals/outcome objectives
- Develop an ongoing system for program improvement

4.2 Special Considerations Regarding Documentation

Many programs have faced various challenges documenting IPS cases and efforts. Different programs document their IPS efforts in various ways. Additionally, not all areas use STD Management Information System (STD*MIS; a free database application provided by the CDC to state and local STD control programs for use in managing their disease control programs).

4.2.1 The Creation of Logs Specific for IPS

Tracking Internet partners through STD*MIS is possible, although it requires that data be entered in a unique and timely manner. We have included examples on how Massachusetts and Washington DC track Internet partners through STD*MIS in **Appendix K**. It is recommended that programs create a separate log or spreadsheet that will allow investigation of Internet partners to be initiated and tracked until either enough locating information is obtained to put into STD*MIS or investigation ceases. An example of such a log/spreadsheet is located in **Appendix E**.

Tip from the field
In addition to documenting IPS efforts in STD* MIS,
some program areas have created additional forms to monitor IPS.
See **Appendix E** for an example.

5. Getting Started

While there are common considerations that cover all PN, including IPS, there are also some unique considerations that must be addressed before implementing IPS as listed below. Refer to **Appendix F** for a more complete checklist.

It is important to remember that the websites where patients meet sex partners and from which IPS is being conducted do not have a public health mission. Most of them are private businesses whose primary mission is to generate revenue. It is possible that a health department or CBO presence will be perceived as a threat to that mission. When conducting IPS through a website, it is important to be aware that you are a member of the community and are subject to the rules and regulations of the website. It is imperative to be aware of such rules and regulations pertaining to IPS prior to joining the site.

Rules and regulations regarding Internet interventions will vary from site to site. Some websites will allow one type of Internet effort and not another, for example, they will allow passive outreach, but not IPS. Other websites may require separate profiles for IPS and outreach and will state that they should not be used interchangeably. Being aware of the rules and regulations for each website and following those policies will help to ensure that Internet efforts that are conducted within private businesses are preserved.

5.1 Creating Profiles, Screen Names, and E-mail Addresses

At this stage it should be determined what computer stations and Internet accounts will be used to send and receive e-mails for IPS. Jurisdictions that have already implemented IPS use a dedicated department e-mail account, work-specific e-mails, or have established state profiles for IPS communication. For example, Howard Brown employees who conduct IPS directed at sex partners with e-mail addresses each use their own specific work e-mail addresses, such as employeeX@howardbrown.org. On sites that require profiles (e.g., Manhunt), Howard Brown uses the profile name HBHCinChicago. Washington DC uses the same moniker, dcSTD, for all Internet-based efforts including screen names, profile names, and e-mail addresses (see **Appendix G**). Personal e-mail accounts and profiles should never be used for IPS.

When creating a profile, the official health department logo should be used as the account picture and other identifying information should be filled out respective to ISP/website protocol for health departments. Some websites may require certain information be contained within your profile. For example, Manhunt recently created a standard logo for all profiles conducting IPS or outreach in order to provide a validation of legitimate health-related profiles (see **Appendix H**).

Programs need to be aware that different websites have different options that may help maintain or potentially breach confidentiality. For example, on www.bgclive.com (Black Gay Chat), after creating a profile, it is necessary to choose "My Account Options" and then choose "Turn Who I Recently Visited Off." Otherwise, when an Internet partner's profile is viewed, it will document the health department's visit on that individual's profile.

Tip from the field
IPS should be conducted from designated department e-mail accounts and profiles, and never from personal e-mail accounts or profiles.

Sometimes an e-mail can be sent to an individual within the website. This type of e-mail system is called a proprietary e-mail system and is used by sites such as Manhunt, Adam4Adam, Men4Now, and MySpace.

Anecdotal evidence from experienced programs has found that including specific disease information in proprietary e-mail systems is safe and acceptable to the recipients. In general, proprietary e-mail systems are password-protected, and members of websites designed specifically for sex seeking typically have individual accounts. If members choose to share an account with another person, it is typically because they are in a relationship and looking for group sexual encounters.

5.2 Staffing

Staffing for IPS is dependent upon the organizational structure, program size, STD morbidity, and appropriateness of using IPS for target populations. IPS must be conducted by staff members, typically DIS, who are trained in traditional PN techniques (i.e., have taken courses such as Introduction to STD Intervention and Advanced STD Intervention) and have experience conducting traditional PS. An experienced DIS who is already well-versed in traditional PS methods, protocols, and principles will ensure that basic PS practices are adhered to while conducting IPS.

Other important qualities for DIS implementing IPS should include familiarity with computers, the Internet, and with social networking sites (SNS). DIS should also be acquainted with online populations, including the language, etiquette, and culture of chat rooms and other current, popular sites. They should have experience with the language and culture of the populations offline (e.g., African-Americans, youth, or MSM).

Professionalism and the ability to separate personal from professional activities are essential.

Given that IPS is a new area for disease intervention, the STD program manager may want to establish this function as a lead position, using an experienced DIS. As increased use of this new venue for disease intervention increases over time, this function may become routine for all DIS within a program.

Tip from the field

Massachusetts Department of Public Health's STD Division has found that having one experienced DIS conduct IPS was preferable to having all DIS perform IPS. They believe that centralizing this function will assist with quality assurance.

5.3 Training

Effective implementation of IPS comes from the combination of a good candidate, appropriate supervision, and a comprehensive training program. For IPS to be successful, STD/HIV programs will need to provide staff with additional training specific to using the Internet for PS. DIS should be provided with ongoing support because this area is still developing, new technologies are emerging, and websites are constantly changing.

Following is a list of trainings that may be necessary to implement IPS:

- Health department-specific IPS policies and procedures. Some examples include:
    - Revising the interview format to include questions about on-line partners.
    - Setting up online profiles.
    - Reviewing standardized online correspondence and discussing any additional interaction between DIS and patients.
    - Going over scenarios other programs have experienced doing IPS.

- Basics of the Internet – including but not limited to: types of web-based networks (Internet service providers, websites, chat rooms, IM services, etc.) and Internet terminology and iconography.

- Training on chat rooms including chat room terminology and etiquette and finding relevant chat rooms and named partners.

- Cultural competency training, including how and why people use the Internet for sex seeking.

- Internet safety and confidentiality - IPS staff should understand the different security and confidentiality levels of the various modes of online communication, such as e-mail (including proprietary e-mail) and IM.

- Hands-on website experience.

New IPS staff should spend time exploring websites frequented by target populations in order to gain familiarity with how these sites work and to understand these sites from a public health perspective. Surfing the Internet should be an ongoing activity, as more websites will be pulled into the process once all DIS begin asking all patients about Internet partners.

5.3.1 Training for Adjunct Staff

Other program staff should also attend trainings on IPS as needed. For example, all staff answering phones should be instructed on how to answer calls from patients contacted via the Internet. Front-line staff, such as reception or check-in staff at STD clinics, should also know how to interact with patients contacted through IPS.

5.4 Supervision

Effective supervision will reduce the likelihood of error, demonstrate the program's commitment to quality assurance, and reduce risk of misuse of the Internet.

Supervisors should have access to all exchanges made between DIS and the initiated partner, as well as interview records and IPS logs. Supervisors should maintain a list of all IPS-related passwords and screen names. Additionally, support regarding specifics of online interactions should be offered regularly, such as during DIS meetings.

6. Implementing Internet Partner Services

6.1 Original Interview

As with traditional PS, the index patient, also known as the original patient (OP), is an individual who has a laboratory-confirmed STD and, based on program policies, will be interviewed by DIS and offered PS services.

The CDC's Program Operation Guidelines states:

> "While interviewing the patient, the DIS should make every attempt to enlist the patient as a resource, making it clear that the information the patient provides will be confidential and very helpful to the DIS, the patient, and the patient's partners. The DIS can incorporate elements of patient-centered counseling by acknowledging and treating the patient as a partner in reducing additional STD in their community. The partnership

should be clear to the patient."[9] (Partner Services section, p. PS-5)
http://wwwdev.cdc.gov/std/Program/partners.pdf or
http://wwwdev.cdc.gov/std/Program/partner/3-PGpartner.htm

During the interview, DIS should ask OPs whether or not they meet sex partners online. If the OP meets partners through the Internet, ask for the websites used and for screen names, e-mail addresses, and regular descriptive and locating information for all partners. It may be helpful to prompt the patient by naming a few popular sex venues, including websites, bathhouses, and public sex venues, to let the patient know that the DIS is familiar and comfortable with such venues. For case management and future disease surveillance purposes, it is important to acquire the OP's own screen names and e-mail addresses. This will assist in case management as partners name back the OP in cluster interviews. Furthermore, in future cases, if the OP's screen name is provided as a partner, complete locating information will already exist in the database and IPS will not need to take place—traditional PN can instead be initiated.

6.2 Initiating Contact Using IPS

Prior to initiating IPS, DIS should attempt to obtain the geographic location of the individual they are trying to contact. This is often listed in the individual's online profile. Knowing the geographic location of the sex partner allows the DIS to provide appropriate referral information (i.e., clinic locations, clinic times). If a partner can be located based on an address or telephone number, those avenues should be used prior to conducting IPS. IPS is traditionally conducted if other methods fail to elicit a response or if it is the only information available. Some programs are looking to use IPS concurrently, such as contacting a partner by phone, while simultaneously trying to contact the same person through IPS. Data regarding this practice are not yet available.

6.2.1 Out-of-Jurisdiction Considerations

E-mail addresses and screen names with an identified geographic location outside of a program's jurisdiction will require that an "out of jurisdiction" (OOJ) field record be initiated. Because the Internet does not adhere to jurisdictional boundaries, traditional methods of handling OOJ contacts may need to be adjusted when conducting IPS. Geographic boundaries are not often able to be adhered to in IPS. Rather, it is important to discuss the situation with the STD program in the jurisdiction in which the partner is known or alleged to reside to understand that jurisdiction's protocols for handling IPS. Until more is known about the standards of practice in each state, or national guidelines are developed for OOJ IPS, these situations will need to be handled on a case-by-case basis. In areas where patients and partners frequently cross jurisdictions, it is recommended that STD programs in these areas work together to develop standard protocols for addressing OOJ-IPS partners. For example, the New England states have formed a regional agreement with Massachusetts serving as the lead project area and performing IPS for all states except for New Hampshire, which has its own IPS program. In these circumstances, Massachusetts sends an e-mail to the OOJ partner on behalf of the applicable jurisdiction. The e-mail contains the contact information of a DIS in the

relevant jurisdiction (where the partner resides). Massachusetts will then create a file for this case but will not enter it into STD*MIS. Rather the partnering state should enter the case into their case management system.

In other areas, Washington DC, for example, the health department will contact the OOJ and will transfer the case, if the jurisdiction is able to conduct IPS. If not, DC will offer to conduct IPS on behalf of the jurisdiction. Additionally, DC will discuss IPS with the OP in order to determine confidentiality. With the jurisdiction's permission to proceed and with the consent of the OP, DC initiates IPS and signs any correspondence with the DC DIS contact information.

6.3 Types of Notifications

6.3.1 Notification via DIS

This notification strategy allows DIS to take responsibility for notifying partners for whom they have an e-mail address, screen name, or IM account.

Currently, there are two ways in which e-mails notifying potentially infected partners of their exposure are written. The first way mimics traditional PN referral letters and is more conservative and lacks specific exposure information. These messages stress the importance for immediate communication between the potentially infected individual and the DIS due to "an urgent health matter" (see **Appendix H** for traditional e-mail examples). The second method is more specific and provides more detailed information about why the partner is being contacted. These messages state that the partner may have been exposed to an STD and urge the partner to contact the DIS or to seek medical care ASAP. This method is typically used only on websites with proprietary e-mail systems or on sex or dating sites and not for IPS sent to general e-mail accounts; although a few programs, such as DC, use this type of language for all IPS (see **Appendix I** for alternative e-mail examples).

In general, initial IPS messages should consist of a brief message encouraging the partner to contact the DIS either by e-mail, telephone, or face-to-face.

Subsequent attempts to contact the partner may include, where appropriate, additional information to increase the sense of urgency; request for the individual's consent to receive information via IPS, disease-specific exposure information, etc.

At a minimum, all IPS messages must include the following information: name, program or health department affiliation, office address, office phone number, and times the DIS can be reached in the office. It may also be helpful to mention that leaving a message on voicemail is confidential, if this is indeed the case. All correspondence should include directions on how the patient can confirm the contacting individual's identity, such as including the name of a supervisor and his/her telephone number. Additional referral information may be included, such as: instructions to present the IPS

message at a medical care location, as well as the names, addresses, and phone numbers of testing and treatment sites, and the hours of service.

All IPS letters should be sent from a health department/CBO e-mail address or profile. The ability to confirm that the IPS is not a hoax but a real and urgent matter is very important for the patient. Whenever possible, messages should be accompanied by an automatic request for notification when the message is read.

Programs must also determine the allowable number of times a patient may be contacted. Experienced programs recommend no more than three attempts to initiate contact with the patient. Some websites have policies regarding the number of times a health department or CBO may contact their members. Manhunt's policy is that no more than two attempts to initiate communication with a patient be made per disease exposure event (see http://www.ncsddc.org/docs/FinStgdWorkingManhunt.pdf). It is important to remember that each situation may require different strategies (see **Appendix J** for a detailed description of when DC sends IPS e-mails).

San Francisco has reported great results, anecdotally, by having computers in the interview rooms. If a patient mentions that he/she meets partners on an Internet site on which the health department has a profile, the DIS will immediately log on to that site and ask the patient to help the DIS find their sex partners. DIS then offer to send an IPS e-mail to all sex partners via the city clinic's profile without mentioning the OP, though, on occasion, the OP will want to send IPS emails to their partners from their personal profiles. They have found that this approach helps to normalize the use of the Internet as a way to find partners.

6.3.2 Notification From The Original Patient

6.3.2.1 Personal IPS

This notification strategy allows for the infected individual to notify their partners of their exposure to an STD via IPS. With assistance from DIS, infected patients will receive support and guidance about how to contact their sex partners on the Internet. Patient-initiated IPS messages should include the name and contact information of the DIS to contact at the health department. Some health departments have found IPS to be more successful when the OP makes first contact with named partners, with follow-up by DIS, as compared to the DIS making first contact.

6.3.2.2 Via Third-Party Sites

Third-party websites, such as InSpot.org, allow patients to notify their partners, anonymously or not, of a possible exposure to an STD. There are limited outcome evaluation data available on these third-party notification sites, currently most data are web usage statistics; however, these sites have potential to improve or increase PS for

STDs such as Chlamydia and gonorrhea, which often do not fall with in the purview of PS. Los Angeles County launched InSpotLA in December 2005. In 2006, the first full year of regular operation of the website, a total of 9,916 e-cards were sent to 15,984 recipients. Broken out by infection, most of the e-cards sent were about crabs and scabies, followed by Chlamydia, gonorrhea, and HIV. The great majority of e-cards (83.7%) were sent anonymously, but nearly as many (80%) also contained a personal message; 24.5% of e-card recipients clicked through to the inSPOTLA website to receive more information.[22]

Sites such as InSpot.org make it very easy for people to notify their partners on their own for STDs for which DIS don't traditionally get involved. However, for STDs such as HIV and syphilis, the DIS model is still recommended because there is no way of verifying that a partner was actually notified, or that the individual sending the notification even has a laboratory-confirmed STD.

6.4 IPS Patient Follow-Up

It is currently within the purview of each jurisdiction to establish policies on IPS follow-up. The following are suggested procedures to consider.

- When a partner calls or comes to the clinic, ask how he/she was notified of his/her potential exposure. If the individual was notified via IPS, the DIS may not have the real name of the individual. DIS should ask the individual for his/her Internet screen name or e-mail address, then search the case management data system, e.g., STD*MIS (**Appendix K**). Once the DIS confirms the identity of the individual through other locating information obtained from the original patient, update the field record. Do not delete the screen name or website from AKA section.

- Print and attach to the field record all IPS correspondence with the date and time sent.

- Some individuals may consider seeking services from private medical providers. When individuals respond with this plan, the DIS should offer to contact the private medical provider on behalf of the patient. Often, the DIS is able to get an individual's case expedited for medical care in the physician's office. It also allows the DIS to reiterate the recommended examination, testing, and treatment protocols with the private medical providers. Health departments will want to be sure that private medical providers are following recommended STD treatment guidelines and are properly treating exposed individuals.

6.5 Special Considerations

6.5.1 Instant Messaging

There will be occasions when an investigator has only an individual's screen name associated with a specific IM program. If it is not possible to send a private e-mail, the

DIS needs to determine if the use of IM is an appropriate mechanism for providing PS since there are numerous variables that can potentially breech a partner's confidentiality. For example, IM conversations can be viewed by website owners and managers as well as health department IT staff. Or IMs can go straight to a cell phone. Additionally, some IM programs will sit on a computer desktop whether or not the account user is present. This means that anyone can see an IM when it pops up on the computer screen and, therefore, anyone can respond to the IM as well.

7.0 Future of IPS

As new technologies become available and are adopted by the general public, the field of public health will want to adjust the way in which we conduct business, prevent the spread of disease, and reach our target populations. There will be many future technologies that will facilitate sex seeking and currently there are two technologies, mobile phones and social networking sites (SNS), that health departments and program areas should begin to think about and consider using for IPS. However, to date, there is no published evidence or knowledge about how to conduct IPS via these mediums.

7.1 Cell Phones

Much like the Internet, mobile phone use has become commonplace in the US. Currently, 73% of adults, 77% of young adults, and 63% of teens own cell phones[23] and 33% of cell owners use the text-messaging features on their phones.[24]

Moreover, cell phones are replacing landline telephones. A report released in April 2007 by the CDC found that about 15.8% of American homes did not have landline telephones but most of those households had at least one working wireless telephone. Half of those Americans living in households with only wireless phones are less than 30 years of age. Wireless-only adults are more likely to be living in poverty. They are also more likely to be men, Hispanic, and living in the South.[25]

It can also be expected that Internet access via mobile devices will become more prevalent over the next few years. dotMobi is the first Internet domain developed solely for Internet access through mobile phones. Backed by leading Internet and mobile organizations, .mobi allows users to bypass the constraints of operators, handsets, and geography to effectively reach their audience.[26] In fact, .mobi has recently announced that 650 city names will be available to city governments in an effort to offer important city information to citizens and tourists. The city sites will be ideal for sharing news information, giving business updates, promoting culture and events, and accessing local attractions, services, and transportation.[27]

Mobile technologies like cell phones are changing the way in which we contact people, which has relevancy for PN. Currently, we are unaware of any programs or health departments in the US that are using cell phones specifically for PN; however, there is one published case out of the UK. In 2001, a letter to the editor in the journal

Sexually Transmitted Infections described a clinic patient presenting for STD testing at a health clinic due to a text message sent to him from his girlfriend. The text message included the woman's clinic number and a diagnosis of trichomoniasis. As a result, the man was able to receive appropriate treatment. This case suggests that mobile phones and text messaging should be considered for PN.[28]

7.2 Social networking sites (SNS)

SNS have gained widespread popularity in both the US and worldwide. In 2007, the Pew Internet and American Life Project reported that approximately 55% of teens between the ages of 12 and 17 use online SNS such as MySpace (www.myspace.com) and Facebook (www.facebook.com). Forty-eight percent of these teens reported accessing these sites on a daily basis or more often.[23] MySpace is by far the most popular SNS with 85% of the respondents reported having a MySpace profile. And it's not just teens; 20% of adults have also created a profile on a SNS site[23] and the numbers continue to grow. From 2005 to 2006, MySpace alone saw a 367% year-over-year growth rate in profiles created.[29]

Needless to say, SNS can be another online venue for sex seeking. Anecdotally, we know that people are finding sex partners on these sites, and that people testing positive for STDs are naming partners for which the only information they have is a SNS profile. However, at the writing of these guidelines, we know of no health department or program that has actually conducted PN on a SNS, but there are program areas that are starting to think about the specifics and logistics of conducting IPS on these types of sites.

8.0 Summary

Internet Partner Services (IPS) provides a unique set of tools that can facilitate the contact of potentially infected individuals. Currently, IPS is most valuable in contacting individuals that may otherwise be unreachable through screen names, e-mail addresses, or other Internet aliases. In most jurisdictions, IPS is being used as a supplement to traditional PN but, as experience grows and as the technology evolves and is employed by public health, IPS has the potential to become the preferred method of PN.

The need for guidance in regards to IPS has been well established; both the Division of STD Prevention and the Division of HIV Prevention at the CDC encourage the use of the Internet for STD/HIV prevention, including IPS.

These guidelines have been created to assist program managers in the development of their IPS activities or to enhance any existing guidelines. Developed from program experience and lessons learned by state departments and nonprofit CBOs, these guidelines provide a foundation to build on and are not prescriptive. It is anticipated that each jurisdiction will use this guidance as a foundation in the creation of local guidelines that can address their needs, capabilities, policies, and procedures. Before implementing IPS, programs must adhere to applicable state/local laws, regulations, and statutes.

The content of these guidelines provide guidance on how the Internet can be best used to contact individuals exposed, or potentially exposed, to an STD/HIV. Current national STD and HIV program guidelines provide a set of shared principles for the provision of STD partner services and HIV counseling and referral services. These principles remain in effect and applicable when using the Internet for PN.

Documentation, program evaluation, process measures, outcome measures, and other forms of data collection and program review are critical to the long-term success of IPS.

The guidelines address concerns such as confidentiality, ethics, computer security, staffing, training, and supervision. It is understood that there are significant barriers to the use of IPS in some jurisdictions that make IPS a unique challenge. Obstacles such as approved access to Internet sites that are traditionally blocked and the engagement of key stakeholders exist. With the development of these guidelines it is hoped that these obstacles will be overcome. In addition to this guidance, consistent and informed supervision will help to ensure that many of these concerns are addressed.

To ensure that partner notification is effective in its mission to reduce STD and HIV transmission, public health must employ new technologies as they are adopted by the general public. These guidelines will help to ensure that your use of the Internet for PN is as effective and productive as possible.

References

1. Centers for Disease Control & Prevention (2008). Guidelines for HIV/STD Partner Services. Draft version 01-10-2008.

2. Klausner, J.D., Wolf, W., Fischer-Ponce, L., Zolt, I. and Katz, M.H. (2000). Tracing a Syphilis Outbreak through Cyberspace. JAMA. 284: 447-449.

3. Centers for Disease Control & Prevention. (2003). Internet Use and Early Syphilis Infection Among Men Who Have Sex with Men --- San Francisco, California, 1999—2003. MMWR. 52(50): 1229-1232.

4. Centers for Disease Control & Prevention. (2004). Using the Internet for Partner Notification of Sexually Transmitted Diseases --- Los Angeles County, California, 2003. MMWR. 53(06): 129-131.

5. Bender, M., Gerard, A., Clothier, W., Wills-Hooks, B. and Goldberg, M. (2002, March). Using E-mail as an Investigative Tool in Syphilis Case Management. Paper presented at the National STD Prevention Conference, San Diego, CA.

6. Constant, P. (2004, March). Utilizing the Internet for Partner Notification. Paper presented at the National STD Prevention Conference, Philadelphia, PA.

7. Gratzer, B., Pohl, D. and Cummins, J. (2007, July). Internet Partner Notification: Outcomes from a community-based DIS program. Poster session presented at the International Society for STD Research meeting, Seattle, WA.

8. Mimiaga, M.J., Tetu, A.M., Gortmaker, S., Koenen, K., Fair, A.D., Novak, D.S., VanDerwarker, R., Bertrand, T., Adelson, S. and Mayer, K.H. (2008). HIV and STD status among MSM and attitudes about Internet partner notification for STD exposure. Sexually Transmitted Diseases. 35(2): 111-116.

9. Centers for Disease Control & Prevention. (2001). Program Operations Guidelines for STD Prevention. Atlanta, GA. Retrieved June 13, 2007, from http://www.cdc.gov/std/program/default.htm#guidelines

10. Centers for Disease Control & Prevention. Revised Guidelines for HIV Counseling, Testing, and Referral. Published November 9, 2001 for MMWR. 50 (No. RR-19): 1-58. http://www.cdc.gov/mmwr/preview/mmwrhtml/rr5019a1.htm

11. Centers for Disease Control & Prevention. Revised Recommendations for HIV Testing of Adults, Adolescents, and Pregnant Women in Health-Care Settings. Published September 22, 2006 for MMWR. 55 (No. RR-14): 1-17. http://www.cdc.gov/mmwr/preview/mmwrhtml/rr5514a1.htm?s_cid=rr5514a1_e.

12. McFarlane, M., Bull, S.S. and Rietmeijer, C.A. (2000). The Internet as a newly emerging risk environment for sexually transmitted diseases. JAMA. 284(4): 443-446.

13. McFarlane, M., Bull, S.S. and Rietmeijer, C.A. (2002). Young adults on the Internet: Risk behaviors for sexually transmitted diseases and HIV. Journal of Adolescent Health. 31 (1): 11-16.

14. McFarlane, M., Kachur, R., Bull, S. and Rietmeijer, C. (2004). Women, the Internet, and sexually transmitted infections. Journal of Women's Health. 13 (6): 689-694.

15. Klausner, J.D., Levine, D. and Kent, C. (2004). Internet-based site-specific interventions for syphilis prevention among gay and bisexual men. AIDS Care.16 (8): 964-970.

16. Gilliam, J., Augustine, J. and Penn, A. (2003). Web-based interventions for youth at risk for HIV/STDs. Presented at the STD/HIV Prevention and the Internet conference. Washington, DC.

17. Levine, D.K., Scott, K.C. and Klausner, J.D. (2005). Online syphilis testing – confidential and convenient. Sexually Transmitted Diseases. 32 (2): 139-141.

18. Madden, M. (2006, April). Internet Penetration and Impact. Pew Internet & American Life Project. http://www.pewinternet.org/PPF/r/182/report-_display.asp

19. Douglas, J. and Janssen, R. (2005). Dear Colleague Letter – the Internet, risk behaviors and potential interventions. Centers for Disease Control & Prevention, September 13, 2005. http://www.cdc.gov/std/DearColleague9-13-2005.pdf

20. Centers for Disease Control & Prevention. HIPAA Privacy Rule and Public Health. Atlanta, GA. Published April 11, 2003 for MMWR. 52: 1-12. http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

21. Salabarria-Pena, Y., Apt, B.S. and Walsh, C.M. (2007). Practical use of program evaluation among sexually transmitted disease (STD) programs, Centers for Disease Control and Prevention, May 17, 2007. http://www.cdc.gov/std/Program/pupestd.htm

22. Rotblatt, H., Plant, A., Levine, D., Engeran, W.J. and Kerndt, P.R. (2007, July). The First Year of inSPOTLA: Report from the Field on Internet HIV/STD Partner Notification. Poster session presented at the International Society for STD Research meeting, Seattle, WA.

23. Raines, L. (2007, February). The new digital ecology: The growth and impact of the Internet (and related technologies). Presented at the Washington Web Managers Roundtable, Washington, DC. http://www.pewinternet.org/ppt/2007%20-%202.1.07%20-%20Webmanagers%20Roundtable%20-%20final.ppt

24. Rainie, L. and Keeter, S. (2006, April). How Americans use their cell phones. Pew Internet & American Life Project. http://www.pewinternet.org/PPF/r/182/report_display.asp

25. Blumberg, S.J. and Luke, J.V. (2007, May). Wireless substitution: Early release of estimates based on data from the Nation Health Interview Survey, July – December 2006. National Center for Health Statistics. http://www.cdc.gov/nchs/nhis.htm

26. dotMobi. (2006). .mobi fact sheet. Retrieved 9/21/2007 from http://www.mydotmobi.com/about_whatisdotmobi.htm

27. dotMobi. (July 9, 2007). Dotmobi offers "city.mobi" names. Retrieved 7-9-2007 from http://pc.mtld.mobi/node/679

28. Newell, A. (2001). A mobile phone text message and *Trichomonas vaginalis*. Sexually Transmitted Infections. 77: 225.

29. Neilson/Net Rating. (2006, May). Social networking sites grow 47 percent, year over year, reaching 45 percent of web users. http://www.nielsen-netratings.com/pr/pr_060511.pdf

Glossary of Acronyms

AKA	Also known as
CBOs	community based organizations
CDC	Centers for Disease Control & Prevention
DSL	digital subscriber line
DIS	Disease Intervention Specialist
EDG	Employee Development Guide
FAQ/A	Frequently Asked Questions/Answers
GLI	Group Level Interventions
HC	health communications
HERR Guidelines	CDC Guidelines for Health Education & Risk Reduction Activities
HIPAA	Health Insurance Portability and Accountability Act
IM	Instant Message or Instant Messaging
IO	Internet Outreach
I&R	Information and Referral
IT	Information Technology
ILI	Individual Level Interventions
IOP	Internet Outreach Programs
IPN	Internet Partner Notification
IPS	Internet Partner Services
ISP	Internet Service Providers
ISIS	Internet Sexuality Information Services
LGV	*Lymphogranuloma venereum* (an STD)
MSM	Men who have sex with men
MMWR	Morbidity & Mortality Weekly Report (CDC)
MRSA	Methicillin-resistant *Staphylococcus aureus* infection
NCI	National Cancer Institute
NGOs	Non-governmental organizations
NCSD	National Coalition of STD Directors
OP	original patient
OOJ	out of jurisdiction
PN	Partner Notification
POG	Program Operating Guide
PCRS	Partner counseling and referral services
PS	Partner Services
SNS	social networking sites
STD*MIS	STD Data Management Information System

For a more comprehensive list of acronyms used on the Internet please click:

http://www.gaarde.org/acronyms/

APPENDIX A

Examples of Confidentiality Agreements

Example #1 – Howard Brown Health Center

PLEDGE OF CONFIDENTIALITY

It is the goal of Howard Brown Health Center (HBHC) to provide our clients (anyone seeking care or services with or through HBHC) with professional, competent and quality care and education in a respectful, affirming atmosphere. As an employee, consultant, auditor or volunteer of HBHC, you have a responsibility to maintain a sense of concern and professionalism while performing your duties. In the execution of this duty, you must be sensitive to the comfort, sensitivities and confidentiality of the client.

The comfort and confidentiality of our clients is of primary concern to HBHC. The professionalism of our staff is necessary to maintain the comfort and trust we have built through the years. Courts and health care professionals maintain that upholding patient confidentiality is an absolute necessity. Federal Courts guarantee absolute privacy regarding all STD medical records. Furthermore, sexual health histories may not be subpoenaed by any court. Breaches of confidentiality regarding the aforementioned data may be punished by dismissal. As an employee, consultant, auditor or volunteer of the HBHC, it is imperative that you follow all Federal, state and local confidentiality laws.

In addition to the legal confidentiality laws, as an employee, consultant, auditor or volunteer of HBHC, you must also abide by the following:

- Some of us, in the context of our duties, advise, within the clinical setting, appropriate and inappropriate behavior as it pertains to physical and/or mental wellness. In the context of this document, clinical setting includes all areas and/or physical space in which you perform your assigned duties.
- We do not, and can not, be "moral custodians", nor do we have policing rights.
- Do not discuss clients or client data with unauthorized persons.
- Discuss clients or client data only to conduct legitimate business, and such discussions should take place only in a manner(s) and location(s), which affords absolute privacy.
- Do not discuss clients or patients outside of HBHC for any reason.
- Make no reference to a client visit to HBHC should you meet a client elsewhere.
- Preserve the confidentiality of friends who are HBHC clients as you would any HBHC client.
- Never acknowledge the presence or absence of clients to any caller.
- Respect for clients is mandatory as a representative of HBHC.
- Client confidentiality is respected and maintained by all staff and other members of the Howard Brown Health Center's workforce after concluding their working relationship with Howard Brown Health Center.

BREACH(ES) OF CONFIDENTIALITY WILL NOT BE TOLERATED AND IS GROUNDS FOR IMMEDIATE DISSMISSAL.

We guarantee our clients absolute confidentiality of their records. Any client requesting a copy of their records must follow the HBHC Policy of Chart Access. No person shall be permitted to view client medical, mental health, or case management records, unless written documentation of permission by the client involved is provided.

Your signature below confirms that you have read, understand and accept to follow the Howard Brown Health Center's Pledge of Confidentiality.

Signature: _____

Name: _____
Date: _____

Example #2 – San Francisco Department of Health

CONFIDENTIALITY AGREEMENT

USE OF DPH RECORDS AND INFORMATION SYSTEMS

Individuals with access to the records and information systems (Internet, e-mail, telephone, pager, fax machines, etc.) of the San Francisco Department of Public Health have a legal and an ethical responsibility to protect the confidentiality of medical, financial, and personnel information, and to use that information and those systems only in the performance of their jobs. The following rules apply to information that you receive or send from any source, including computer, paper, telephone, and facsimile.

Confidential information may not be accessed, discussed, or divulged in any form except as required in the performance of your duties. Sharing confidential medical information is allowed within DPH among medical professionals in order to provide medical care to a patient.

You may not use any DPH information system for any type of personal use. Use the following test: "Is my use of this information system enabling me to provide better service, or to perform my duties more effectively or less expensively?" If the answer is no, then your use of the information or system is unnecessary and/or inappropriate.

Be aware that most DPH information systems maintain records of what is viewed and/or sent by whom. You may be asked to justify why you viewed or released specific information.

You may be given a user ID and a password to enable you to view computerized information. Under no circumstances may you disclose your User ID or password other than to your supervisor or to IS staff. If you suspect someone else has knowledge of your password, you must immediately notify your supervisor and the divisional IS Manager.

The hardware, software, and data used in the DPH information systems are the property of DPH. All software installed on a DPH computer must be authorized in writing by IS and must be licensed to allow installation on a DPH computer. DPH has the right to review and remove personal or unlicensed software and data on any DPH computer.

If you, inadvertently or intentionally, misuse or improperly disclose your user ID or password, misuse or improperly disclose confidential information, use DPH information systems for personal reasons, or install personal or unlicensed software or data on a DPH computer, you may lose access to the computer system, be subject to disciplinary action up to and including termination, be reported to the appropriate licensing board, and/or be subject to civil or criminal liability.

****
****

I understand that I have no privacy right in the information in my DPH computer or the information that I access or send via my computer or other DPH equipment. I acknowledge that my use of DPH information systems and equipment may be monitored.

_____	_____
PRINT NAME	**DIVISION**
_____	_____
SIGNATURE	**SSN**

Appendix B

Example of a Legal Disclaimer

Notice

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this e-mail in error please notify the sender. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

Appendix C

Protocol for the use of a stand-alone computer with DSL line

Reasons for a specifically dedicated computer:

Research has shown that people are not only using the Internet for seeking sex partners but that these online behaviors are often antecedents to very risky offline sex behaviors, including increases in anal sex and a decrease in condom use. Activities such as online outreach, partner notification, and health communications are additional public health tools for STD/HIV prevention and education.

Approved activities:

- Access to sexually explicit websites and content on the Internet
- Access to chat rooms
- Access to social networking sites
- Use of instant messaging programs
- Use of web-based e-mail programs

Unacceptable activities:

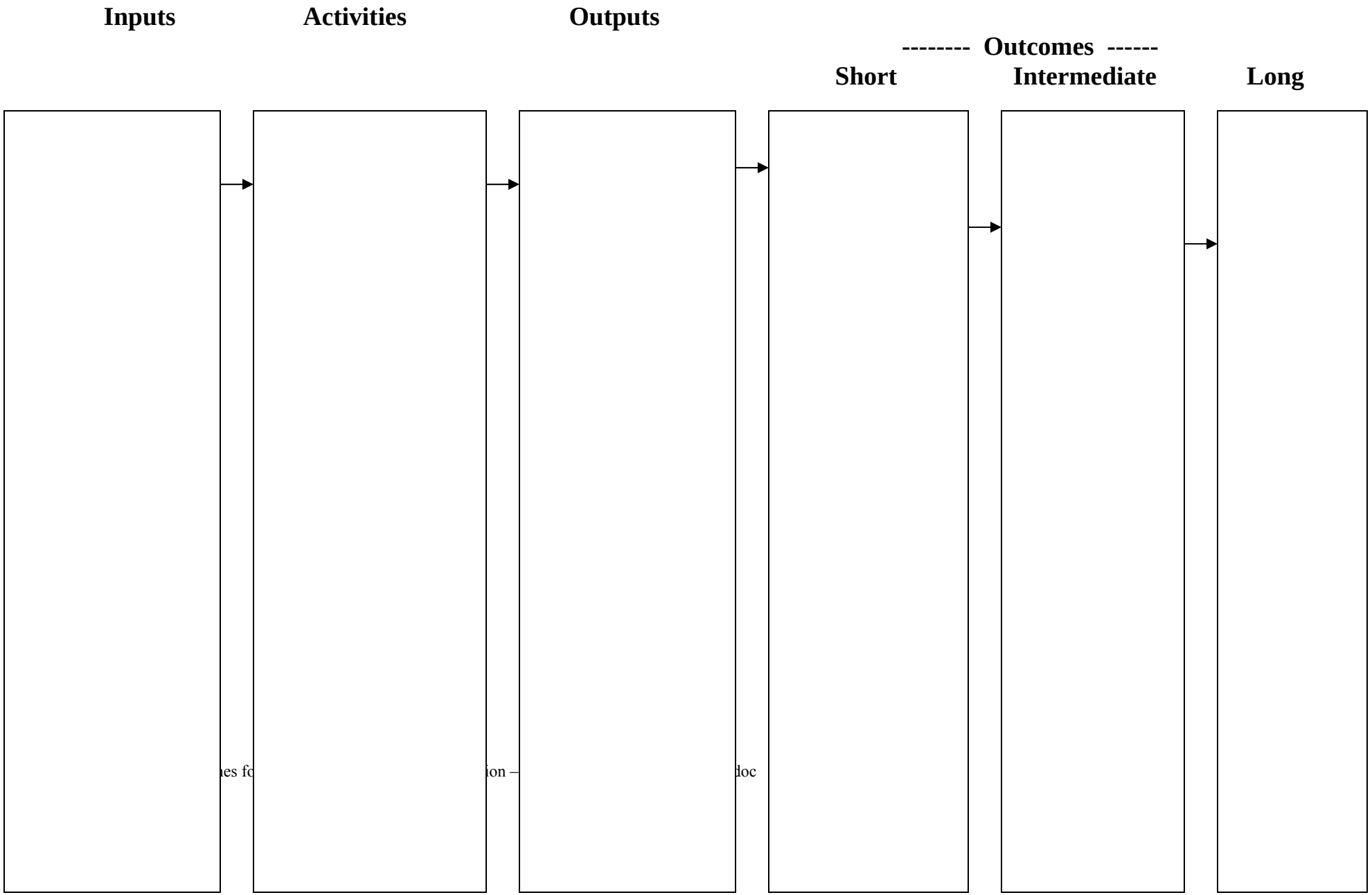
- Gambling
- Dating
- Downloading non-work-related music or videos
- Illegal activities

Computer access:

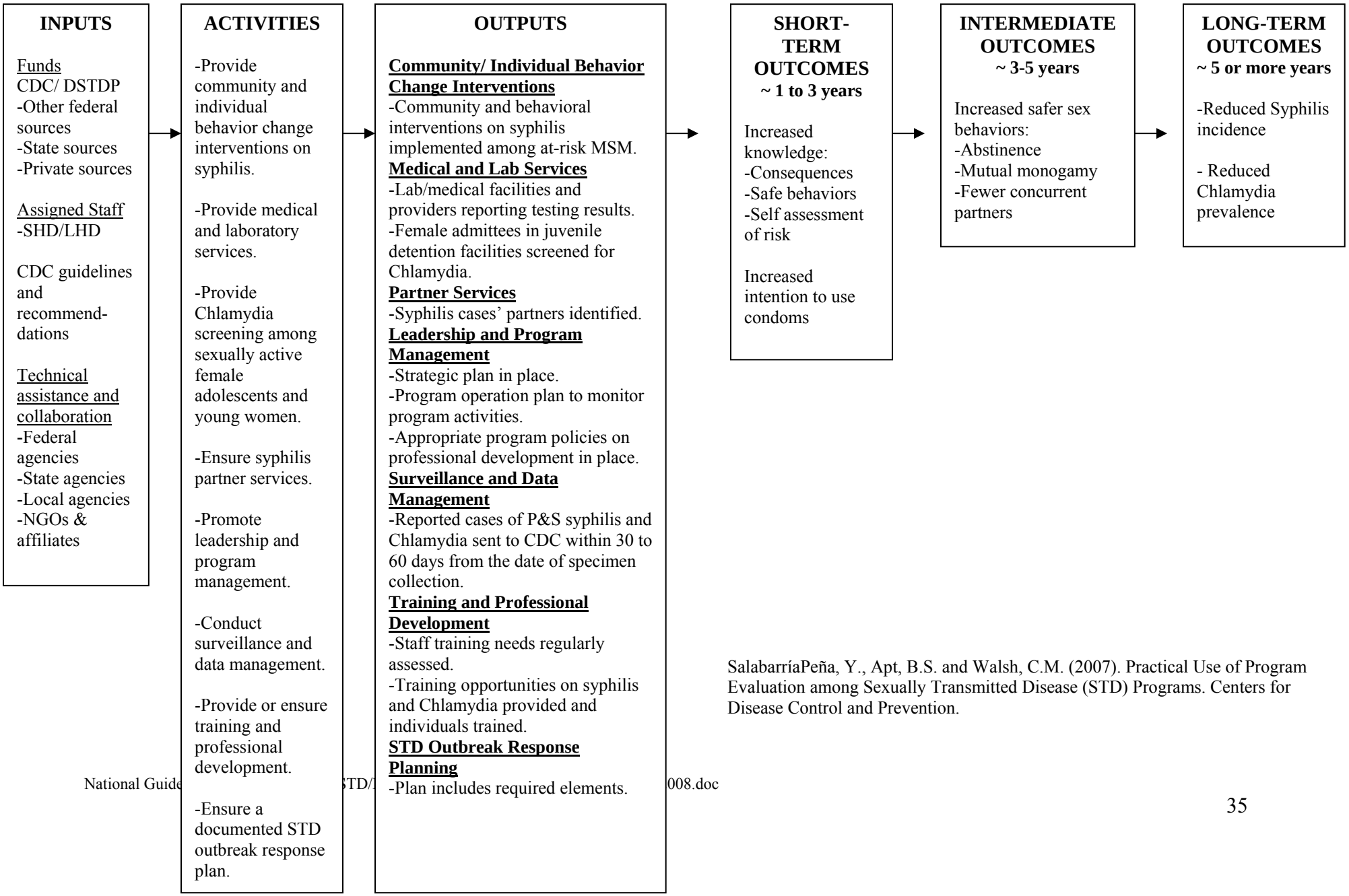
- Researchers whose work specifically relates to the Internet (or other technologies) and STD/HIV prevention may use the dedicated computer
- The computer will be password protected
- All researchers with access to the computer will have to sign a form agreeing to use the computer only for the approved activities
- The computer will be maintained on a unique server that has no connection to the main server
- The computer will have virus protection that will be regularly updated.

APPENDIX D
Logic Models
Logic Model Template

Goal/Situation:



Logic Model for State X Comprehensive STD Prevention Systems (CSPS) Program



SalabarríaPeña, Y., Apt, B.S. and Walsh, C.M. (2007). Practical Use of Program Evaluation among Sexually Transmitted Disease (STD) Programs. Centers for Disease Control and Prevention.

APPENDIX E

Example of Documentation Log

INTERNET PARTNER NOTIFICATION LOG SHEET

Your Name: **DIS # & State:**
Initiation Date: **OP Id # and Disease:**

Partner #	E-Mail Date	Website Name	Partner's E-Mail	E-Mail Script #	AM Logon Time	PM Logon Time	Notes/Outcome of Activity	Disease Verification (3rd E-mail)	Closure Code
1									
2									
3									
4									

APPENDIX F

Check list for creating guidelines for online/Internet partner notification

☐ Determine who will need to be involved with the creation of the guidelines
- ___ Health Department Medical Director/Administrator
- ___ Health Department Security Coordinator
- ___ Health Department Information Technology (IT) Director
- ___ Legal Department
- ___ Management Information Systems (MIS) Director
- ___ STD Epidemiologist
- ___ STD Area Managers
- ___ STD Program Managers
- ___ HIV Program Managers
- ___ STD Disease Intervention Specialist (DIS) representative
- ___ External Partners (community-based organizations [CBOs] working with affected communities, Website owners, etc.)

☐ Determine who will be covered by the guidelines
- ___ A specific department (e.g., STD/HIV program)
- ___ A city or county health department
- ___ The entire state department of health

☐ Determine technological and staffing needs
- ___ Do you need to hire someone new or are there existing staff members who can work on Internet/online projects such as partner notification online?
- ___ How much of this staff member's time will be dedicated to online projects – 5 – 100%?
- ___ Should this staff member come to the position with the necessary knowledge or can they be trained on the job?
- ___ Is there someone who has the time to supervise this staff member?
- ___ Is there at least one computer that can be dedicated to this purpose?
- ___ Creation of a dedicated e-mail account?
- ___ Approval obtained for unrestricted access to the Internet?
- ___ At least one IT contact working with staff member?

☐ Sections of guidelines
- ___ Introduction/Purpose
- ___ Involved personnel
- ___ Description of responsibilities of all involved personnel
- ___ Competencies required of personnel conducting online partner notification
- ___ Training
- ___ Confidentiality
- ___ Standard Operating Procedures of conducting online partner notification including templates and examples

___ Adverse Events or Emergencies
___ Documents and Documentation
___ Evaluation

Details within each Guideline section

☐ Introduction/Purpose
___ Statement of purpose, i.e., who, what, when, where, why
___ Description of chat rooms, instant messaging, listservs, websites, etc., as well as passive vs. active outreach

☐ Personnel intimately involved with the online partner notification
___ Primary employee conducting online partner notification
___ Secondary employee to cover if primary employee is out of the office
___ Supervisor
___ IT employee for guidance and technical support

☐ Description of responsibilities of all involved personnel

☐ Competencies required of personnel conducting online partner notification
___ Demonstration of good judgment and performance of responsibilities related to partner notification
___ Cultural Competency

☐ Training (some examples/suggestions)
___ Introduction to STD Intervention (ISTDI)
___ Information Security Training
___ Internet Partner Notification and Referral Services Training

☐ Confidentiality
___ Description of how confidentiality will be handled and maintained
___ Description of how a patient's identity will be confirmed
___ Confidentiality agreement signed by all involved parties including IT and front-desk staff

☐ Standard Operating Procedures of conducting online partner notification including templates and examples
___ Creation of step-by-step procedures on how to conduct online partner notification
___ Creation of documentation forms and logs
___ Creation of e-mail language, number of attempts made in a certain time frame, etc.
___ Creation of referral resources
___ Templates of e-mails, forms, logs, etc.

☐ Adverse Events or Emergencies

___ Description of how adverse events or emergencies will be handled
___ Who will handle adverse events or emergencies?

☐ Documents and Documentation
___ List of all documents to be used including copies
___ Where documents will be stored
___ When and who will review documents
___ Documents should include, at minimum, the following:
___ original patient case number
___ e-mail or screen name of partner
___ website where partner was met, if possible
___ real name of partner if obtained
___ disposition of the case
___ dates & times e-mails were sent
___ responses received
___ turn-around time or time frame for completion

☐ Evaluation
___ **Process Evaluation** (ongoing evaluation while program is being developed and implemented)
___ During development and implementation, meet on a regular basis with the team involved and ask the following questions:
- What is working?
- What should be improved?
- How should it be changed?

___ **Outcome Evaluation** (assessing the degree to which the program has met the objectives, or the degree to which the program has been of use to the target population)
___ Outcome evaluation should be conducted yearly to gauge the impact of the program. Ask the following questions:
- What has happened?
- Who was affected?
- What was the most effective aspect of the program?
- Was it cost-effective?

Appendix G

Examples of Screen Names and Profiles

Organization	Screen/Profile Name	Email address
San Francisco City Clinic	SFCityClinic	johnd@sfdph.org
Massachusetts Dept. of Health, STD Division	DivofSTDMA	Varies
Howard Brown	HBHCinChicago	johnd@howardbrown.org
Washington, DC STD Control Program	dcSTD	dcSTD@dc.gov

Required Manhunt Logos for Health-Related Profiles

Example 1: Massachusetts Department of Health, Division of STD Prevention Partner Notification Profile

Example 2: Washington, DC STD Control Program
Partner Notification Profile

Example 3: Legacy Community Health (Houston, Texas)
Outreach Profile

APPENDIX H

Sample e-mails - Traditional language

Day 1 of Investigation
E-mail - 1st attempt
To: SexKitten@sexsite.com
From: StarDIS@ncsddc.org
Subject: URGENT HEALTH MATTER

My name is John Investigator, and I am with NCSD. I have urgent and confidential health information to discuss with you. I can be reached at my office at (555) 234-5678. Please contact me as soon as possible. Thank you, John Investigator.

Day 3 of Investigation
E-mail - 2nd attempt
To: SexKitten@sexsite.com
From: StarDIS@ncsddc.org
Subject: HEALTH DEPARTMENT MATTER
My name is John Investigator and I work with NCSD. I attempted to contact you on 01/01/04; I have some very important health information to share with you. This is a very urgent matter, and because of the confidential nature of this information, it is vital you contact me. Please call me at (555) 234-5678. I can be reached at this number from 8am to 5pm, Monday through Friday or you can contact me using my e-mail address StarDIS@ncsddc.org or my cell phone at (555) 255-5888. To assist you in confirming my identity, I have included my supervisor's name and phone number: Josefina Boss, Program Manager, (555) 234-5679. Please do not delay in contacting me.
John Investigator
Disease Intervention Specialist
NCSD
South Central District Office (555) 234-5678

If no response after Day 4, the DIS should discuss the situation with their supervisor. Attempt to re-interview the original patient for additional locating information, and/or consider having the original patient attempt to notify the partner. The original patient can explain that a representative from the health department will be contacting him/her with important health-related information, plus provide the DIS name and office number.

Appendix I

Sample e-mails - Alternative language

E-MAIL 1

Day 1 of investigation
Dear <<screenname>>,

My name is John Doe, and I am from the Washington DC Department of Health, STD Control Program. I'm emailing you because someone you met online was recently diagnosed with a laboratory-confirmed sexually transmitted disease (STD).

You need immediate medical attention because this person identified you as a sexual partner during the infectious period of this STD. For confidentiality reasons, I cannot tell you anything about the person you had sex with, including when it occurred.

Please call me at 202.XXX.XXXX, and I can tell you more about the specific infection and where you can go to be tested and treated for free.

If I'm not there when you call, I will call you back. Be sure to leave a number and time when I can reach you. My voicemail is private, confidential, and password-protected.

I check my voicemail and email at the beginning and end of each business day (8am-4:30pm, M-F).

If you want to check that this email is real, call the Division of STD Prevention at 555-555-5555 and ask to speak with our Medical Epidemiologist, Dr. J. Doe. You can also <<call Website/ISP Administration at XXX.XXX.XXXX>> to confirm the legitimacy of this <<Website/ISP] account.>>

Thank you,

John Doe, [credentials]
Disease Intervention Specialist (or other title)
STD Control Program, Washington, DC Department of Health
Email: dcSTD@dc.gov

E-MAIL 2

Day 6 of Investigation
Dear <<screenname>>,

I noticed that you read my first email, but I didn't hear back from you.*

I have important information about the specific STD you have been exposed to and want to give you a couple of ways to get this important information:

1. You can call me at 202.XXX.XXXX and I can tell you more. My voicemail is private, confidential, and password-protected.

2. You can email me (at this email or at dcSTD@dc.gov), and let me know that it's okay to give you more details about this STD in writing. Just put "I agree" in the subject line.

Remember, I check my voicemail and email at the beginning and end of each business day (8am-4:30pm, M-F).

[If you want to check that this email is real, call the Division of STD Prevention at 555-555-5555 and ask to speak with our Medical Epidemiologist, Dr. J. Doe. In addition, you can email me at my work address: dcSTD@dc.gov. You can also <<call Website/ISP Administration at XXX.XXX.XXXX>> to confirm the legitimacy of this <<Website/ISP>> account.]

Thank you,

John Doe, [credentials]
Disease Intervention Specialist (or other title)
STD Control Program, Washington, DC Department of Health

If it is not known if the individual read the email (i.e. Adam4Adam), the first line will need to be modified: "A few days ago I sent you an email, and I didn't hear back from you."

If it can be confirmed that the partner has not deleted the first email (which has verification information), then the verification information should not be included in Email 2.

E-MAIL 3

Day 11 of Investigation
Dear <<screenname>>,

As you know, I've tried to reach you twice now about your exposure to a laboratory-confirmed STD. Although I respect that you don't want to contact me to find out which specific infection you may have been exposed to, my hope is that you have visited your medical provider and let them know I've been in contact with you.

Remember, with many STDs, you need to be treated for your exposure, regardless of your STD test result.

This will be my last unsolicited email to you regarding this specific exposure. However, in the future if you are exposed to another laboratory-confirmed STD, I may be contacting you again.

Finally, if you decide to call me (202-XXX-XXXX) or email me (dcSTD@dc.gov), I want to emphasize that our communication is strictly confidential.

Thank you,

John Doe, [credentials]
Disease Intervention Specialist (or other title)
STD Control Program, Washington, DC Department of Health

Appendix J

Description of Washington DC's timeframe for sending IPS e-mails

A series of emails has been created to initiate Internet Partner Notification (IPS) in a standardized manner. The IPS DIS will commence by sending E-mail 1. If there is no response, E-mail 2 shall be sent after five days; likewise, E-mail 3 shall be sent five days later. Only three unsolicited e-mails shall be sent per disease exposure. If the partner expresses interest in no further communication, E-mail "Negative Response" shall be sent. If a partner expresses interest in learning more via e-mail, E-mail "Positive Response" shall be sent. If the interested partner has not responded within one week after E-mail "Positive Response" being sent, E-mail "Positive Response Follow-up" shall be sent. In many situations, partners may attempt to call the IPS DIS, at which point the IPS DIS shall refer to previous training to handle telephone communication.

APPENDIX K

Documenting IPS in STD*MIS

Example - Massachusetts

Documentation Requirements

- The DIS will document all Internet activity.
- DIS must document all work with the date, time and description of each interaction on the Internet PN Log Sheet.
- All e-mail documentation should be kept in a case file.
- Internet PN must be entered and kept up-to-date in STD*MIS (see below).

Entering Internet Screen names into STD*MIS

This section of the policy seeks to address sexual contacts of infected individuals who are known to the infected patient by their screen names or e-mail addresses only. This flexible approach is based on how much information is available about a partner and serves as a systematic way to maintain accurate records of not just names, addresses and phone numbers, but also screen names. In this way, we can perform searches for individuals by their screen names and/or e-mail addresses when no other information is available.

- Individuals who are only known by their screen name are entered into STD*MIS as: Internet, screen name (For example, Internet, Sexyperson.) Both the first and last names should be updated when more information becomes available.
- Screen names are entered into the Also Known As (AKA) section. AKAs should never be changed or deleted. New screen names must be added as needed. (It is important to note that individuals can be searched for in STD*MIS by their AKA only- no other information about first or last names is needed to perform a search.) If the individual is not currently in the STD*MIS system, we can add them and open a new Field Record.
- Screen names pertain to specific Internet sites. These sites (Manhunt, AIM, Yahoo, etc.) must be noted in the Notes section of the Field Record. Individuals may change their screen names frequently, so it is essential that the date of the last known use of the screen name be noted in the Notes section. (For example: MH "Sexyperson" 4/19/06, Yahoo "SexyP" 4/19/05, AIM "SexyPER" 4/19/04.)
- The way we currently manage missing locating information remains the same. For example, if we know a client's first name and address, this individual is entered into the system as "John UNK." Now, with this new system for entering names into STD*MIS, sexual contacts will be entered into the system as "Internet, screen name," or, if we know the client's first name, "John Internet."
- Case dispositions should be entered into STD*MIS with the following codes (STD*MIS does not allow numbers to be entered after letter codes; this can be noted in the case file):

Code	Description
A*	Preventative treatment (not infected - confirmation of examination and/or treatment)
C*	Infected, brought to treatment (infected - confirmation of examination and/or treatment)
L1**	Patient states examination and/or treatment (not infected - no provider confirmation)
L2**	Patient states examination and/or treatment (infected - no provider confirmation)
J**	Informed of disease exposure - no further contact with MPDH (located, received specific STD exposure info, no further contact with MDPH)
H1	E-mails read but never responded (located but refused to respond, did not receive specific STD disease information)
H	E-mail(s) not read (unable to locate)

* Infers direct contact with DIS
** Infers e-mail or phone communication without disclosure of identifying information

Example – Washington DC

Within 72 hours of the Original Interview, the investigating (Ix) DIS will record in the OP's STD*MIS file that the OP had a "PARTNERS INTERNET" risk factor. Internet partners are recorded as contacts of the OP; if a partner is not listed in STD*MIS (after a search using the FIRST NAME, LAST NAME, and AKA fields), a patient record is created for him/her. The Ix DIS should then complete a Field Record for the partner with all information pertaining to the Internet partner (including physical descriptions, identical spelling of e-mail addresses, sex venues, etc.). The Ix DIS will then assign this partner to the IPS Coordinator (writing the IPS Coordinator's Worker Number STD*MIS number in the Field Record).

For data entry, Ix DIS should follow this format:

Individuals who are only known by their screen name (internal e-mails) or e-mail address (external e-mails) are entered into STD*MIS as FIRST NAME: "<<SCREENNAME@WEBSITE or e-mail address>>", LAST NAME: "INTERNET". Both the first and last names should be updated when more information becomes available. The screen names will be entered followed by the website. Note: For long screen names or e-mail addresses, simply enter as much of the name that will fit into the space (20 characters).

Examples for Internal Emails:

Website	Screenname	STD*MIS Entry
Manhunt.net	SWEATYnDC	SWEATYNDC@MANHUNT.NET
Adam4Adam.com	SWEATYnDC	SWEATYNDC@ADAM4ADAM.COM
Manhunt.net	HOTnSWEATYnDC	HOTNSWEATYNDC@MANHUNT.COM
Adam4Adam.com	HOTnSWEATYnDC	HOTNSWEATYNDC @ADAM4ADAM.COM

Examples for External Emails:

Website	Screenname	STD*MIS Entry
Gay.com	SWEATYnDC	SWEATYNDC@GAY.COM
Yahoo.com	SWEATYnDC	SWEATYNDC@YAHOO.COM
Gay.com	HOTnSWEATYnDC	HOTNSWEATYNDC@GAY.COM
Yahoo.com	HOTnSWEATYnDC	HOTNSWEATYNDC@YAHOO.COM

In addition, screen names and e-mail addresses are entered into the AKA section. AKAs should never be changed or deleted. New screen names must be added to the AKA section as needed. (It is important to note that individuals can be searched for in STD*MIS by their AKA only—no other information about first or last names is needed to perform a search.) If the name of the Internet partner becomes known at a later date, it is important that the screen name is moved to the AKA section because it will allow for the individual to be searched in the future under his/her screen name.

Individuals may change their screen names frequently, so it is essential that the date of the last known use of the screen name be noted in the Notes section (e.g., "SWEATYnDC@MANHUNT 4/19/06").

The way we currently manage missing locating information remains the same. For example, if we know a client's first name and address, this individual is entered into the system as "JOHN UNK." Now, with this new system for entering names into STD*MIS, sexual contacts will be entered into the system as "<<SCREENNAME@WEBSITE>> INTERNET" (or "<<EMAIL ADDRESS>> INTERNET") or, if we know the client's first name, "<<FIRST NAME>> INTERNET."

For data entry, IPS DIS should follow this format:

Within the Field Record, under "EVENTS", the IPS DIS shall choose the last option: "INTERNET PARTNER NOTIFICATION". In the "INTERNET PARTNER NOTIFICATION" screen, there are a series of Y/N fields. The first field, "IPS", indicates whether the individual is an Internet partner. The remaining 13 fields, "IPS_L1a through IPS_L4" allow for further explication of the "L" disposition that is designated for an Internet partner (see Dispositions below).

Case dispositions should be entered into STD*MIS with the following codes (STD*MIS does not allow numbers to be entered after letter codes; this can be noted in the case file):

Code	Description
A	Preventative treatment
B	Refused preventive treatment
C	Infected, brought to treatment
D	Infected, not treated
E	Previously treated for this infection
F	Not infected
G	Insufficient information to begin investigation
H	Unable to locate
J	Located, refused examination
K	Out of Jurisdiction
L	Other*

L1 Informed of specific STD exposure (2nd e-mail, phone call, in-person communication)

a. Informed of specific STD exposure, claims preventive treatment
b. Informed of specific STD exposure, refuses preventive treatment
c. Informed of specific STD exposure, claims to be infected and treated
d. Informed of specific STD exposure, claims to be infected and not treated
e. Informed of specific STD exposure, claims to be previously treated
f. Informed of specific STD exposure, claims to not be infected
g. Informed of specific STD exposure, no further contact

L2 Informed of an STD exposure (first e-mail)

L3 Not informed of STD exposure

Refused—E-mails not read even though patient logs in
Refused—Patient blocks IPS screen name
Not known if e-mails are read
Unable to locate (Patient has not logged in during Field Investigation period.)

L4 Insufficient information to begin investigation (Screen name does not exist.)

*The L disposition will be used for Internet disposition codes, provided the Internet partner does not have any physical locating information (i.e., name and/or address). If physical locating information is acquired at any point throughout IPS, traditional disposition codes (A-K) shall be used.

Data Entry into the Proposed STD*PAM

In the proposed STD*PAM software, data entry will follow the same format. However, an additional, "Internet Partner" Disposition Code (e.g., "WI") will be added to differentiate Internet partner dispositions from traditional partner dispositions:

Code	Description
A	Preventative treatment
B	Refused preventive treatment
C	Infected, brought to treatment
D	Infected, not treated
E	Previously treated for this infection
F	Not infected
G	Insufficient information to begin investigation
H	Unable to locate
J	Located, refused examination
K	Out of Jurisdiction
L	Other
W	Marginal Partner Dispositions
WI	Internet Partner Disposition
WI1	Informed of specific STD exposure
WI2	Informed of STD exposure
WI3	Not informed of STD exposure
WI4	Insufficient information to begin investigation

In addition, another question will be added to the field record to indicate the type of Provider (DIS) Referral. The choices will be:

Telephone
In-person
E-mail
E-card