

### Large- Scale Deployment Factors

The purpose of a pilot project is to discover what works well and what does not. For this pilot, a number of valuable lessons were learned and deployment issues identified. The issues are discussed below in three categories: infrastructure, training, and IT support of the mobile technologies.

Infrastructure concerns include connectivity and hardware specifications. Connectivity refers to how the mobile technologies connect to the central database. The laptops needed a connectivity solution that enables caseworkers to connect and sustain access to CONNECTIONS. Connectivity solutions may combine various wireless infrastructures (local hotspots or LAN's, wide area cellular provider services, etc.), and wired infrastructures (in courts and schools). Connectivity for the laptops was not uniformly reliable and faces considerable technical problems because of the densely built environment in much of the city. Cellular connectivity was a major concern with the telephonic dictation service as well due to unreliable cellular service coverage, which led to relatively large numbers of dropped calls and dead-zones (limited or no connectivity). Reliable connectivity is crucial to the success of both the laptop and dictation service strategies. Dealing with these infrastructure concerns must be a core part of future strategies.

Hardware specifications are similarly important. This pertains mainly to the voice recognition software deployed on caseworkers' desktop computers. The software is a relatively complex software application that requires considerable computing power to operate effectively. IT administrators must ensure that computers operating the software have ample processor speed, sufficient memory, and adequate sound cards to meet or exceed the products' minimum requirements.

The digital pens require using special paper in order to convert the analog information to digital text. Although the device is a one time cost, the special paper will be an on going cost to all Local Districts that deploy this technology.

The second main deployment area concerns training for caseworkers. Many of the problems described above are linked to three training needs: (1) basic training dedicated to familiarizing caseworkers with the particular problems and skills required for mobile technology, such as setting-up and calibrating the specific devices and applications, and understanding how to operate them, (2) what is needed to adapt the work practices and the technology capabilities to the work requirements and incorporate it into their daily tasks, and (3) what is needed to troubleshoot the mobile technology in the event that an error or malfunction occurs.

Caseworkers had more difficulties when they were required to learn new skills to use the mobile technologies effectively, particularly with dictation. Training sessions devoted to skills and techniques that enhance caseworkers' ability to dictate their notes may have improved the overall success of the mobile technology. Some caseworkers required additional training for use of the voice recognition software, which requires users to calibrate the software so that it is capable of recognizing users' personal speech patterns and accents.

A greatly expanded mobile technology operation for CPS work will require improvements in the technical and support infrastructure and resources. The districts do not currently have adequate personnel and technical resources to manage large numbers and wide varieties of mobile technologies while caseworkers are in the field. IT support varied from one district to the other, but they all have limited capabilities to support a wide-scale deployment of mobile technologies. The lack of IT support for caseworkers using the voice recognition software led to frustration. And IT support is not limited to providing technical support to caseworkers with mobile technologies, but includes the full range of physical and organizational resources to ensure the systems are working as intended.

### Security

Much of the data caseworkers collect must remain confidential. Security provisions for older paper based systems are not adequate for digital technologies. Security measures exist on several levels, namely data security in repositories or networks, security of data transmission, and security of data in portable devices. The following is a brief overview of the security concerns for each district using these categories.

The security concerns associated with the voice recognition software were related to the devices needed to make the technology portable (digital recorder or a laptop). Existing security technologies are not capable of securing the data on the digital recorder or digital pens. If such devices are used to store identifying information (names, addresses, social security numbers, etc.) the data is subject to loss or theft. When digital recorders or digital pens are connected to a PC for downloading, however, those PC's are parts of networks that may be vulnerable. Data

## Overall Deployment and Security Considerations

---

can be encrypted on the PC, but not on the other portable devices. Allowing work with these devices at home increases all of these risks, particularly if workers use their home PC's for part of the process. The integrity and security of those home PC's are virtually impossible to ensure or maintain.

All three security concerns are applicable to working with connected laptops. The laptops that were deployed during the pilot were capable of connecting to the Internet and public networks. The data was secured on the laptops by requiring caseworkers to have a series of logins and passwords. The data connections were secured by use of a secure socket layer (SSL), a commonly-used protocol for managing the security of data transmission over a network. While several measures were taken to secure the storage and transmission of data, the existing infrastructure did not secure the devices themselves. The laptops' hard drives that were used during the pilot were not encrypted, and did not have a central "kill switch" that could be triggered in the event that a laptop was lost or stolen.

The security concerns with the third party transcription service provider were different from the other technologies. Data was transmitted in two different phases. The first was when the caseworker called into the system and the second was when the caseworker retrieved the typed progress notes from the Web site. Caseworkers reported being very careful of their surroundings when calling in their progress notes to ensure privacy of the data. There was virtually no security concerns related to the transmission of data over the cellular provider's network. And no confidential data are stored on the phone. Initially there were concerns about how the digitized notes on the service provider's servers were encrypted, how they were secured, and what the login protocol was for retrieving the digitized notes from the Web site. In the end, all involved parties reviewed the service provider's policies and accepted the security measures taken. Finally, caseworkers accessed the typed progress notes from the service provider's Web site using their desktop computer in the office (that had basic security measures such as password protection and SSL communications), and copied and pasted them into CONNECTIONS. However, workers could also access the service provider's database from their home PC's, opening a wide range of security risks such as storing sensitive information on a non-agency device. This still needs further investigation.

---