Defining and assigning roles and responsibilities for the surveillance system you plan to build, modify or buy represents an important aspect of planning your program. Today, many jurisdictions have expanded the role of central IT services to include managing IT-related contracts, procuring systems, supporting networks and managing security. Given this expansion, defining roles and assigning responsibilities becomes particularly important so that everyone is clear on expectations, and perhaps even to inform development of a Service Level Agreement (SLA).

The roles identified below and mirrored in the companion worksheet may not fit your program perfectly; some roles may be irrelevant, while others important to your program may be missing. The information and guidance provided for each role is intentionally generic. Modify the worksheet as needed in terms of roles and actors and use it to systematically think through all the potential roles and responsibilities in terms of who owns overall *responsibility* (marked as "R"), owns *implementation* (marked as "I"), and serves in a *support* role (marked as "S").

Development and management of Data Sharing Agreements

Your surveillance program should develop and manage data sharing agreements (DSAs) in close partnership with your program's attorney or legal office. Typically your legal office approves, and perhaps may even sign, all DSAs. Never assume that a DSA from another program will work for you. Clarifying legal authority (see the tool in the *Clarifying Legal and Policy Issues* section of the toolkit) is a critical first step when developing a DSA, as you may discover that your authority may be one of several key differences between your program and another seemingly similar program (see also *Preparing to Meet with Your Attorney* in the *Clarifying Legal and Policy Issues* section).

Vendor contract management

Responsibility for developing and managing vendor contracts varies by jurisdiction; central IT, a separate vendor contract office, or individual public health programs may manage all IT contracts, depending on the dollar amount of the contract. If you do not manage your own vendor contract, consider the unit that does to be a strategic partner to you and your program.

Regardless of who manages the contract, your program must be closely involved in defining the Statement of Work (SOW). You own the requirements (see the tool for *Defining and Validating Requirements* in the section titled *Analyzing Technical Options*) for your system, so only you can say when system functionality meets your needs or not. Just as "good fences make good neighbors," you could say, "good contracts make good partners." Make sure your requirements and SOW are clear, and don't assume that the vendor intimately understands your work or your intentions.

In addition, ensure that you understand any applicable contracting and procurement policies and procedures. You may need to do change orders or amendments if new funding becomes available, so proactively familiarizing yourself with these processes can be useful.

Licensing

As with vendor contracts, software licensing and fees can be managed at different levels. However, management occurs within a central IT unit. Licensing can apply to front-end user interface software or back-end databases or both.

Unless you are using open source or public domain software, you or central IT likely pay licensing fees directly or indirectly via your vendor. Determine if licensing fees exist and how they get paid so that you can budget appropriately. In addition, determine whether any licensing fees are for a universal license or an individual system license. A universal license makes the software available across your health department, while an individual license likely limits availability to you and your staff. Explore sharing costs through a universal, agency-wide license if appropriate.

Digital certificates bring up an issue somewhat related to licenses. Determine if your provider data sources or your surveillance program pay for annual digital certificates. If so, what process do you have in place for ensuring that providers or the program keeps certificates up to date to avoid interrupting data sharing?

System development or enhancements

As with previously described responsibilities, system development and enhancements may be managed by central IT, a separate vendor contract office, your program, one of your community partners, or another managing unit or entity. Regardless, your program or your community collaborative group must set priorities, define requirements and communicate those to the vendor. You must do so either directly or through your managing unit. You must also insist on a project charter (see the *Project Charter Template* tool in this section) so that you clarify the goals, timelines, roles and responsibilities, deliverables and other key aspects of the program at the project's beginning.

You also need solid project management skills. If the managing unit does not provide a project manager, consider how you can add one (e.g., share with another program to reduce costs). The project manager for the vendor's team cannot serve as a substitute for you having someone to monitor timelines, priorities and budgets.

For both system development and enhancements, make sure you have a tool, such as **Bugzilla,** for tracking and providing visibility to bugs. You also need a point person to assume responsibility for tracking bugs through the bug management cycle. Consider asking what bug tracking tool others in your department use to see if that can be a good fit for your program's needs.

Customizations to a commercial-off-the-shelf (COTS) system can be expensive. Determine required enhancements versus "nice-to-haves" when setting priorities with your team. Keep community-wide standards in mind as you consider any state- or program-specific enhancements.

System Testing

Responsibility for system testing requires you to identify someone who can develop test scripts for new functionality based on your requirements. You also need someone who can conduct user acceptance testing (UAT). Ultimately, you also need to assign someone to sign off that the testing is both complete and that the system works at an acceptable level.

Application hosting and data storage

You need to determine if you will host your application and store your data internally, with central IT, a vendor, in the cloud or with a community partner. Your program may not necessarily store its

data in the same location as the application. These determinations may be important to make when preparing to meet with your attorney.

If you have a vendor, you also need to know if they can get access to the application through virtual private network (VPN) or other means if they need to make updates. Figure out if they must work through a point person in central IT or another managing unit, and the agreement on how that is done.

Other important determinations you need to make include identifying:

- Who has access to the data for addressing data quality problems or other issues?
- Who notifies users if the system needs to be down for maintenance?
- Who takes specific actions if the systems crashes or has unplanned downtime?

Ad hoc reporting

You must decide and outline how to manage the inevitable ad hoc report requests. Identify who will manage them. If you have any doubts as to whether or not a report would be an allowable use of your data, find out if you have a process for legal review. Determine who would write the scripts or perform any other necessary actions to extract and format the data. If that individual is with a vendor or central IT, discover if and how they charge for requests. Establish who validates the data and report before sending it to the requestor, and ascertain if it must face validation given its intended purposes.

Security and disaster recovery

Security increasingly falls within the purview of the chief information officer, chief security officer, central IT organization, or some combination of these individuals and groups. However, your program must confirm that the security requirements you have defined adequately protect the data the program collects, particularly if it includes protected health information.

Clarify if you will use a tape backup or “hot” backup and how long it will take to get the system up and running after a disaster. In addition, you must identify or assign a person to:

- Manage system and data backup.
- Decide on the trade-off between speed of recovery and cost.
- Implement a full or partial restore from a backup and ensure it happens at least once annually.