IT Asset Disposition: A Healthcare Decision-Maker's Guide to Selecting an ITAD Partner

Properly done, IT asset disposition (ITAD) can reduce your risks and deliver a solid return on investment.

eBOOK

DYNAMIC
LIFECYCLE INNOVATIONS

Table of Contents

Introduction

The disposition of information technology assets poses significant — and unique — challenges for health systems, hospitals, clinics, and other healthcare organizations.

A primary concern is safeguarding patient data, in compliance with Health Insurance Portability and Accountability Act (HIPAA) rules. Patient data, as well as sensitive corporate data, resides on a broad range of electronic assets, from computer hard drives, CDs, DVDs, and portable USB drives, to highly specialized medical devices such as implanted cardioverter defibrillators (ICDs).

When decommissioning these assets, how do you ensure that any information they contain doesn't fall into the wrong hands? The consequences of a data breach can be severe, including regulatory fines, restitution, and lawsuits, as well as long-term damage to an organization's reputation. Egregious HIPAA violations may even result in prison time.[1]

The unlawful or unethical disposition of electronic waste (e-waste) can be similarly detrimental. Despite the enactment of strict environmental laws, too many IT assets end up in landfills or are improperly shipped to developing countries. Illegal e-waste disposition may result in steep penalties under the Clean Air Act, Clean Water Act, and other laws.

Moreover, standards for accreditation by both The Joint Commission and Centers for Medicare and Medicaid Services (CMS) include the proper disposal of hazardous wastes, in accordance with federal laws, and compliance with HIPAA rules.

Given these ever-increasing risks, healthcare decision-makers must carefully consider the choice of a vendor to assist with IT asset disposition (ITAD). This guide was created to walk you through crucial considerations for evaluating potential ITAD partners.

The consequences of a data breach can be severe, including regulatory fines, restitution and lawsuits, as well as long-term damage to an organization's reputation. Egregious HIPAA violations may even result in prison time.

Crucial Consideration: Data Security

The large and growing pervasiveness of technology in the healthcare setting has yielded many benefits, both to patient care and operational efficiency. However, the proliferation of technology also creates risks, perhaps none more serious than the threats to protected health information (PHI).

As anyone involved with compliance knows, data breaches involving PHI can result in major fines under HIPAA — up to $50,000 per violation, according to HIPAA Journal. HIPAA rule infractions also can jeopardize accreditation by The Joint Commission and CMS (refer to standards and elements of performance IM.02.01.03 covering the security and integrity of health information). Besides putting compliance and accreditation at risk, violations may lead to negative publicity and diminished community trust in the organization.

IT assets and other electronic devices slated for disposition may be especially vulnerable to data breaches. Accordingly, an ITAD provider must make data security a top priority.

Specifically, your ITAD partner should be able to check all of the following boxes:

- ☐ **Data destruction certifications and standards**

Certifications and standards speak volumes about the ability of your ITAD partner to compliantly remove PHI and other sensitive data from decommissioned devices.

In particular, make sure the vendor possesses National Association of Information Destruction (NAID) AAA Certification®, considered the data security "gold standard" for ITAD vendors. NAID AAA-certified vendors are subject to regularly scheduled audits by trained, accredited security professionals, as well as random unannounced audits. NAID AAA Certification covers employee background screening and training, compliance with written procedures, access controls, operational security, equipment destruction, confidentiality agreements, and transparency for clients.[2]

HIPAA rule infractions can not only result in fines of up to $50,000, but also jeopardize accreditation by The Joint Commission and CMS.

Often considered the data security "gold standard" for ITAD vendors, NAID AAA-certified vendors are subject to regularly scheduled audits by trained, accredited professionals, as well as random unnanounced audits.

Crucial Consideration: Data Security continued

In short, ITAD vendors with NAID AAA Certification have demonstrated the ability to meet or exceed HIPAA requirements for protecting patient information, which is a key element of receiving and maintaining accreditation by The Joint Commission and CMS.

Other important attributes include adherence to National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization (NIST 800-88), which spells out best practices for hard drive erasure, and the Department of Defense standard for sanitization (DoD 5220-22m), which addresses the complete erasure of data from digital media.

Cyber liability insurance

As noted earlier, data breaches can be very costly to healthcare organizations, considering the potential for regulatory fines and payouts to lawsuit plaintiffs. The risks extend to devices that have been handed off to your ITAD partner for disposition. Be sure that your evaluation process includes this question: "Do you carry cyber liability insurance." If the answer is "yes," ascertain whether the coverage is sufficient, based on the partner's industry knowledge and legal/compliance analysis. For example, the sponsor of this guide maintains a $10 million cyber liability policy, along with a financially guaranteed closure plan, to protect the long-term interests of its customers.

Employee background screening

Although it might seem like an internal matter, an ITAD vendor's background screening of all employees protects your interests, and it should be part of your evaluation process. Does the screening include a criminal background check that covers a person's last seven years, consistent with NAID AAA certification requirements? In particular, the vendor should not hire anyone who has a felony conviction for burglary, theft, embezzlement, or fraud. You don't want devices containing sensitive data to fall into the hands of a criminal. Also, if a data breach occurs and the case ends up in court, your defense can point to your reliance on the ITAD vendor's extensive screening process to prevent such an occurrence.

Facility security measures

It may not be your job to evaluate the security of an ITAD vendor's processing facility. However, certain security measures offer strong evidence that the company is serious about protecting sensitive information housed on decommissioned devices. Besides universal employee screening, one telltale indicator is a NAID-compliant network of surveillance cameras that can monitor all access points into secure areas, including "blind spots" inside and outside the facility — wherever confidential media are received, staged, processed, and/or destroyed. In addition, footage from these cameras should be retained and available for review for a minimum of 90 days.

Seek out an ITAD partner that carries adequate liability insurance - **$10 million** for cyber security and **$10 million** for e-waste pollution.

Crucial Consideration: Data Security continued

Accessibility and transparency

Will the potential partner allow you to tour the facility, either in person or virtually? Again, you may not consider yourself an expert evaluator of an ITAD vendor's processing facility. But you may be able to spot warning signs of a less-than-optimal operation, such as large stockpiles of IT equipment, employees who aren't wearing security badges, and work areas that lack organization and clear designations.

Your tour host should make various subject matter experts from operations, data security, value recovery, and other areas of interest available to you for questioning. The most accommodating ITAD vendors may even encourage you to ask frontline employees about their experiences and perceptions of workplace culture.

Timely asset scheduling and pickup

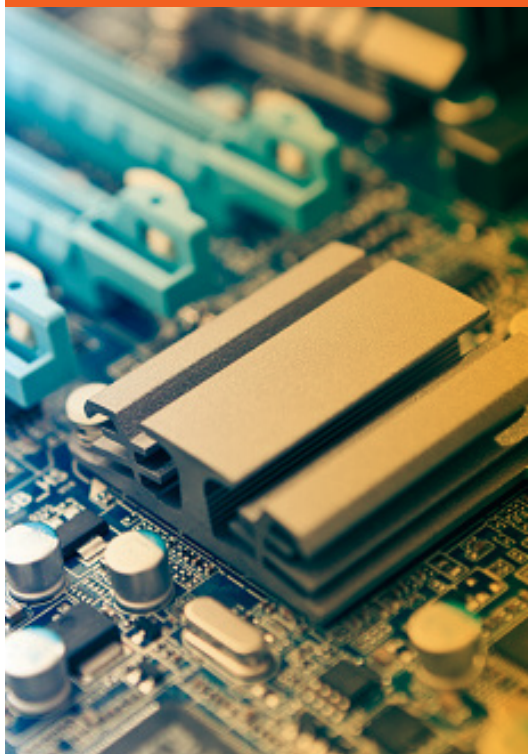
The two most vulnerable times for a data breach are when assets are headed for disposition and upon arrival at the ITAD vendor's facility. To minimize this risk, your partner should be able to accomplish fast turnarounds for pickup scheduling (e.g., within 24 hours) and the actual pickup itself (e.g., within 72 hours). Also, find out whether the ITAD vendor has a designated area to securely hold incoming devices until they can be processed.

Full chain of custody

Naturally, you should be concerned about the security of IT assets and other equipment once they leave your loading dock. However, your ITAD partner can alleviate your concern by assuming full liability for these devices from the time they're picked up at your facility, through receipt, reconciliation, data destruction, hardware refurbishment or end-of-life processing, and the recovery of metals and other commodities…in other words, throughout the full "chain of custody."

Outsourcing of these steps should be kept to a minimum. However, when it is necessary, any subcontractors should have been thoroughly vetted, and they should hold the same certifications and adhere to the same standards as the ITAD vendor.

When vetting ITAD providers, be wary of those who outsource their solutions. The more your data changes hands, the greater the risk of a data breach.



Crucial Consideration: Environmental Compliance

Thanks to ongoing technological innovation, a large and constantly growing array of devices can be found in every corner of today's healthcare facilities. Certainly, devices such as computers, tablets and telecommunications equipment play a key role in achieving operational efficiencies. Advanced technology also benefits patient care. From the emergency department to patient rooms, and everywhere in between, diagnostic and therapeutic equipment helps ensure optimal clinical outcomes.

But what happens to technology when it becomes obsolete or non-functional? For healthcare organizations of all types, good environmental stewardship has become a core objective. This commitment must extend to the proper disposition of electronic devices and the array of hazardous materials they contain — especially considering the public health implications. It's important to understand that outsourcing this task to an ITAD vendor does not shield your organization from costly penalties or reputational damage due to illegal or unethical practices. In this respect alone, the evaluation of ITAD vendors should be conducted with the utmost due diligence.

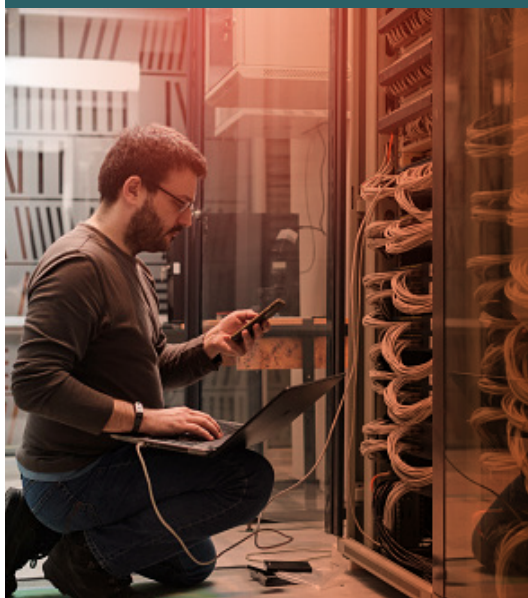
Keep in mind, also, that the proper disposition of e-waste, in compliance with federal and state laws, plays a role in accreditations by The Joint Commission and CMS, as spelled out in the "Environment of Care" standards and elements of performance (EC.02.02.01). Partnering with the wrong ITAD vendor may implicate your organization in violations of these rules and put your accreditations at risk.

The right ITAD partner will check all of the following boxes:

☐ **Environmental certifications**

Certifications by accredited, independent third-party entities provide a clear indication that an ITAD vendor adheres to the highest standards for electronics recycling. Two certifications stand above the rest: Responsible Recycling (R2), managed by Sustainable Electronics Recycling International (SERI),[3] and e-Stewards Standard for Responsible Recycling and Reuse of Electronic Equipment, developed by the Basel Action Network (BAN), a nonprofit organization focused on eliminating toxic trade.[4]

The proper disposition of e-waste, in compliance with federal and state laws, plays a role in accreditations by The Joint Commission and CMS. Partnering with the wrong ITAD vendor may implicate your organization in violations of these rules, putting you at risk.



Crucial Consideration: Environmental Compliance continued

R2 certification spells out environmental health, safety, and security criteria pertaining to the handling of electronics that contain mercury, CRT glass, barium, and other toxic materials. In addition, it prohibits these materials from being incinerated, dumped in landfills or shipped to non-Organization for Economic Cooperation and Development (OECD) countries. Likewise, the e-Stewards Standard forbids transboundary movements of non-functioning IT assets to underdeveloped countries. It also prohibits forced labor and requires annual audits.

Make certain that your ITAD partner actually possesses these certifications. Some providers will state that they "follow," "adhere to," or "are complaint" with R2 and e-Stewards certifications. However, these claims do not ensure full compliance or accountability, exposing your organization to risk.

One more important certification is ISO-14001, developed by the International Organization for Standardization. It establishes an environmental management plan as a part of a healthcare organization's integrated management system (IMS). This certification reflects a commitment to following all environmental laws and best practices for IT asset end-of-life disposition, as well as for workplace safety procedures.[5]

Pollution liability insurance

Illegal dumping and other environmental violations are unlikely if you're partnering with a reputable, certified ITAD vendor. Still, mistakes happen, and all it takes is one mistake to incur steep penalties — potentially tens of thousands of dollars under both the Clean Air Act and the Clean Water Act. Liability can extend beyond ITAD vendors to their clients, which is why your ITAD partner should carry adequate e-waste pollution liability insurance. As with cyber liability insurance, the policy amount should be based on the partner's industry knowledge and legal/compliance analysis (for example, the $10 million pollution liability policy, plus financially guaranteed closure plan, maintained by the sponsor of this guide).

Vetting of downstream vendors

Ideally, your ITAD partner will possess the capability to handle most electronics processing in-house. However, with certain types of assets and materials, such as copper, plastics, and circuit boards, the provider may outsource processing to another vendor. Ask your prospective ITAD partner to provide a list of every downstream vendor by location and type of material processed. Most importantly, make sure that these vendors carry the same certifications, including R2 and e-Stewards, as the ITAD vendor.

Landfill and export policies

Although it's addressed by the previously discussed R2 and e-Stewards certifications, your ITAD partner should have clearly stated policies that no electronics will go into a landfill, nor will they be shipped to non-OECD countries.

In addition to **R2** and **e-Stewards**, the ideal ITAD partner will also hold **ISO-14001** certification, reflecting a commitment to following all environmental laws and best practices for IT asset end-of-life disposition, as well as for workplace safety procedures.

Other Differentiating Factors

While data security and environmental compliance deserve the lion's share of your ITAD evaluation process, other factors can help you differentiate among multiple partner candidates. These considerations speak to return on investment, client visibility into ITAD processes, and logistics and transportation.

The following factors can help further aid in the selection of an ITAD partner:

One-stop convenience

Some ITAD vendors may not be able to process the wide range of e-waste generated by hospitals, clinics, and other healthcare facilities. Ask prospective ITAD partners whether they'll accept items besides IT assets, including highly specialized medical equipment. By partnering with a "one-stop shop," you can realize efficiencies and possibly even cost savings, while reducing the number of trucks backing up to your loading dock.

Meaningful profit-sharing

An ITAD partner's profit-sharing program can help healthcare organizations offset their disposition costs. Larger, well-equipped ITAD providers are often able to repair and refurbish IT assets, such as laptops, desktops, servers, networking equipment, and mobile devices, and then resell them through various channels. Non-resalable devices may contain precious metals and other materials that can be harvested and sold for reuse. Expect your ITAD partner to share at least 50% of the net sale price with your organization. ITAD vendors that rely on multiple channels (retail, wholesale, B2B/direct, broker) generally are able to secure better prices than those that sell through a limited network.

On a related note, your organization may prefer to donate refurbished IT equipment or proceeds from the profit-sharing program to local charities. Ask potential partners about their ability and willingness to customize a donation program that supports your philanthropic mission.

ITAD reporting and customer portal

Full transparency is a hallmark of reputable ITAD vendors that adhere to industry best practices. In fact, they try to make it as easy as possible for their clients to view important ITAD information, such as settlement statements, certificates of recycling and data destruction, audit reports, and remarketing settlement summaries.

Expect your ITAD partner to share at least 50% of the net sale price of remarketed assets with your organization.

Other Differentiating Factors continued

Ideally, your partner can integrate its reporting system with your organization's asset management software via an application programming interface (API). This will simplify and expedite your ability to identify which assets are live or dispositioned, as well as assisting with preparation for internal or external audits and other vital activities.

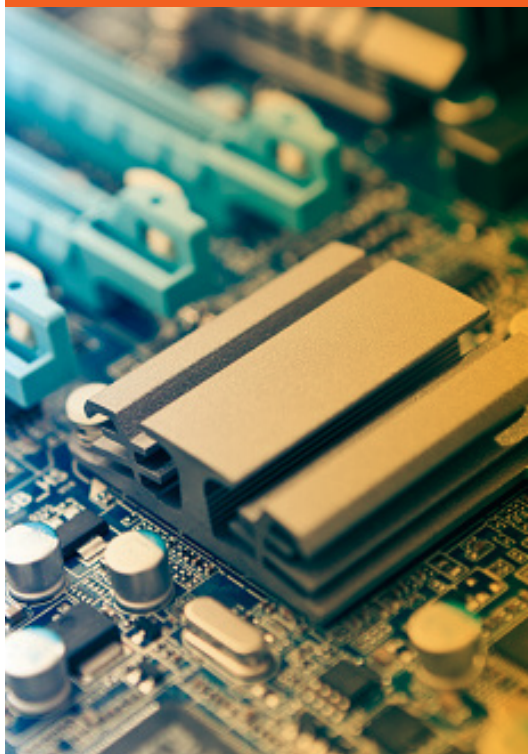
In addition, look for an ITAD vendor that offers an intuitive online customer portal offering broad functionality, such as scheduling pickups; generating automated communications of key milestones, including scheduled, received, and finalized material processing; and producing analytical reports and audit documentation.

Logistics and transportation services

By providing comprehensive logistics and transportation services, an ITAD partner can remove a significant burden from healthcare organizations. Services may include onsite packing, palletizing, and serial number tracking, as well as pickup and transport of the devices. If you have a remote workforce, inquire about the vendor's ability to pick up units from multiple employee locations, using small package services offered by various carriers. Steer clear of vendors that have minimum or maximum quantity requirements.

Of course, you want your equipment to ship as efficiently and cost-effectively as possible. But your ITAD partner should place the highest priority on the security of PHI and other sensitive data throughout the chain of custody. NAID AAA-certification means that the vendor's transportation operations are regulated and audited by the National Association for Information Destruction.

ITAD partners can remove significant burden from healthcare organizations by providing logistics and transportation services.



Summary of Evaluation Criteria

Considering the inherent risks and potential opportunities, healthcare organizations need to carefully evaluate potential ITAD partners. Following is a summary of the crucial considerations discussed in this guide:

Data security

- ☑ Data destruction certifications and standards
- ☑ Cyber liability insurance
- ☑ Employee background screening
- ☑ Facility security measures
- ☑ Accessibility and transparency
- ☑ Timely asset scheduling and pickup
- ☑ Full chain of custody

Environmental compliance

- ☑ Environmental certifications
- ☑ Pollution liability insurance
- ☑ Vetting of downstream vendors
- ☑ Landfill and export policies

Other differentiating factors

- ☑ One-stop convenience
- ☑ Meaningful profit-sharing
- ☑ ITAD reporting and customer portal
- ☑ Logistics and transportation services

About Dynamic Lifecycle Innovations

Founded in 2007, Dynamic is a full-service electronics and materials lifecycle management corporation specializing in IT asset disposition, data security, product refurbishment, remarketing and resale, electronics recycling, legislative compliance, and materials recovery. Dynamic has devoted more than 15 years to working with clients in the healthcare sector, managing their IT hardware and other electronic assets. Our industry-leading chain of custody ensures the protection of sensitive patient and organizational data, while focusing on environmental stewardship, value recovery and service excellence. Dynamic is headquartered in Onalaska, Wisconsin, with an additional facility in Nashville, Tennessee.

Visit thinkdynamic.com for more information about Dynamic. Click here to request a callback from an experienced ITAD professional, or call 608-781-4030.

References

[1] HIPAA Journal, "What Are the Penalties for HIPAA Violations?" tinyurl.com/5n7y8mbm

[2] iSigma International Secure Information Governance and Management Association, tinyurl.com/5fv43p9f

[3] SERI, tinyurl.com/3rvjdjsn

[4] e-Stewards, tinyurl.com/bdevr5hr

[5] ISO, tinyurl.com/2p8d2mm2