

### Print4 Solutions fully comply with all HIPAA regulations

Print4 solutions do not access, store, process, monitor, or manage any patient information. Print4 manages and optimize printer devices and fleets, and while these devices may print patient information, the Print4 software cannot access any information being printed.

Print4 performs scheduled scans of designated IP address ranges to capture meter readings, device supply levels, and/or device alerts. Print4 cannot communicate information about any specific print job.

Communications are controlled by using limited access to the designated IP address ranges. All communications originate from the Print4 Onsite Software Client. Communication of device information outside the network uses a 128 bit SSL with added password protection.

Print4 cannot be configured to perform tasks beyond those the for which software was intended The products can only report device status information for the equipment being monitored.

We understand that network security administrators and IT managers are ultimately responsible for HIPAA compliance of all systems and devices. We designed the system so administrators can be assured that the Print4 Solutions are resulting in no areas of compromised security.



- The HIPAA (Health Information Portability and Accountability Act) of 1996 is a federal law that protects health information.
- Organizations regulated by HIPAA need to ensure they are meeting the standards required by the Act when dealing with third party vendors.
- It is the responsibility of the security officer to ensure the company's compliance with the regulations; no entity exists to give HIPAA certification of a solution.
- Print4 solutions comply with the strictest interpretations of the HIPAA regulations.
- Print4 does not and cannot access patient information.

# IHS HIPAA Security Checklist

## A. Administrative procedures to guard data integrity, confidentiality, and availability

- 1) Certification - 142.308(a)
  - Risk Analysis—Complete Facilitated Risk Assessment (FRA) and analyze results
  - Risk Management—Implement security plans resulting from FRA
  - Security Policy—Review and update as necessary
- 2) A Chain of Trust Partner Agreement - 142.308(a)
  - Establish chain of trust partner agreements with all business partners with which IHS exchanges PHI
- 3) A Contingency Plan - 142.308(a)
  - Applications and Data Criticality Analysis—Complete development
  - Data Backup Plan—Complete review
  - Disaster Recovery Plan—Complete review
  - Emergency Mode Operation Plan—Complete review
  - Testing and Revision Process—Complete review
- 4) Formal Mechanism for Processing Records - 142.308(a)
  - Review and update content as appropriate
- 5) Information Access Control - 142.308(a)
  - Access Authorization—Review and update access authorization
  - Access Establishment—Review and update access definitions
  - Access Modification—Review and update rules for modifying access
- 6) Internal Audit - 142.308(a)
  - Review and update content as appropriate
- 7) Personnel Security - 142.308(a)
  - Assuring supervision of maintenance personnel by an authorized, knowledgeable person—Complete procedure
  - Maintaining a record of access authorizations—Complete procedure
  - Assuring that operating and maintenance personnel have proper access authorization—Develop or update procedure as necessary
  - Establishing personnel clearance procedures—Update procedure as necessary
  - Establishing and maintaining personnel security policies and procedures—Update procedure as necessary
  - Assuring that system users, including maintenance personnel, receive security awareness training—Update procedure as necessary
- 8) Security Configuration Management - 142.308(a)
  - Documentation—Complete security plans, rules, and procedures
  - Hardware and software installation and maintenance review and testing for security features—Update procedures as necessary
  - Inventory—Update inventory as necessary
  - Security testing—Complete procedures
  - Virus checking—Compliant

# IHS HIPAA Security Checklist

- 9) Security Incident Procedures - 142.308(a)
  - Report Procedures—Complete procedures
  - Response Procedures—Complete procedures
- 10) Security Management Process - 142.308(a)
  - Risk Analysis—Will be repeated every three years or upon significant system changes
  - Risk Management—Implement continuous process
  - Sanction policies and procedures—Make a part of the annual security training
  - Security policy—Make a part of the annual security training
- 11) Termination Procedures - 142.308(a)
  - Changing locks—Review compliance as a part of the recurring Risk Analysis
  - Removal from access lists—Review compliance as a part of the recurring Risk Analysis
  - Removal of user account(s)—Review compliance as a part of the recurring Risk Analysis
  - Turning in of keys, tokens, or cards that allow access—Review compliance as a part of the recurring Risk Analysis
- 12) Training - 142.308(a)
  - Awareness training for all personnel, including management personnel—Review compliance as a part of the recurring Risk Analysis
  - Periodic security reminders—Review compliance as a part of the recurring Risk Analysis
  - User education concerning virus protection—Review compliance as a part of the recurring Risk Analysis
  - User education in importance of monitoring log-in success or failure and how to report discrepancies—Review compliance as a part of the recurring Risk Analysis
  - User education in password management—Review compliance as a part of the recurring Risk Analysis

## **B. Physical safeguards to guard data integrity, confidentiality, and availability**

- 1) Assigned Security Responsibility - 142.308(b)
  - No action required
- 2) Media Controls - 142.308(b)
  - Implement changes as necessary
- 3) Physical Access Controls - 142.308(b)
  - Disaster Recovery—Update procedures as necessary
  - An Emergency Mode Operation—Update procedures as necessary
  - Equipment Control—Update controls as necessary
  - A Facility Security Plan—Update procedures as necessary
  - Procedures For Verifying Access Authorizations Before Granting
  - Physical Access—Update procedures as necessary
  - Maintenance Records—Update record content as necessary
  - Need-To-Know Procedures For Personnel Access—Update procedures as necessary
  - Procedures To Sign In Visitors And Provide Escorts, If Appropriate—Update procedures as necessary
  - Testing And Revision—Update procedures as necessary

# IHS HIPAA Security Checklist

- 4) Policy and Guidelines On Work Station Use - 142.308(b)
  - Update existing policy and guidelines as necessary
- 5) A Secure Work Station Location - 142.308(b)
  - Update policy as necessary
- 6) Security Awareness Training - 142.308(b)
  - Update existing policy as necessary

## C. Technical security services to guard data integrity, confidentiality, and availability

- 1) Access Control - 142.308(c)(1)(i)
  - Procedure for Emergency Access—Update the existing policy as necessary
  - Context-, Role-, or User-based Access—Update the existing policy as necessary
- 2) Audit Controls - 142.308(c)(1)(ii)
  - Update audit controls as necessary and implement consistently
- 3) Authorization Control - 142.308(c)(1)(iii)
  - Update authorization controls as necessary
- 4) Data Authentication - 142.308(c)(1)(iv)
  - Develop and implement authentication controls as necessary
- 5) Entity Authentication - 142.308(c)(1)(v)
  - Implement dual factor authentication when feasible

## D. Technical Security Mechanisms

- 1) Communications or Network Controls - 142.308(d)
  - Both of the following:
    - Integrity Controls—Implement new integrity controls as necessary
    - Message Authentication—Implement new authentication controls as necessary
  - One of the following:
    - Access Controls—No action necessary
    - Encryption—Implement for open network transmission
- 2) Implementation Features - 142.308(d)
  - Alarm—Implement new features as necessary
  - Audit Trail—Implement new audit controls as necessary
  - Entity Authentication—Implement two factor authentication as feasible
  - Event Reporting—Implement new tools as necessary

# Print4™ System Specifications

## Hosted Environment

Print4 is an Applications Service Provider (ASP) model that resides within a server farm at our secure Tier III, SAS70 Type II certified hosted facility that is fully staffed 24/7/365. Cisco ASA and PIX firewall appliances are employed as well as basic filtering of ports. The Cisco appliances provide stateful packet inspection, inter-server traffic filtration (DMZ), integrated intrusion detection and Virtual Private Network (VPN) capabilities, among other security features. Additionally, security audits of the servers are performed regularly to ensure the safety and reliability of the systems.

## Application Construction

Both the local Onsite Java Applet and the Discovery Java Applet utilize the latest Java 1.6v. They were intentionally constructed as applets to minimize potential corruption or intrusion within the local host's operating system.

## Application Communication and Operation

**Onsite:** Communication is securely transmitted through SSL port 443. Inbound communication is limited to applet updates that typically last less than 30 seconds once per day and/or at startup. Outbound traffic consisting of meter counts, device service and service contact data is transmitted automatically at a pre defined interval or at the customer request. Outbound communication typically lasts less than 60 seconds. Preferred device scans are limited to the pre-defined Private Community Names, MAC Address, IP Address and / or Subnet ranges loaded within the application and it is incapable of pulling data from anything other the MIB tables of the serial numbered devices that it is searching for.

**Discovery:** Communication happens within the network and only on the network segments specified by the user. Discovery is accomplished using Simple Network Management Protocol (SNMP). The Discovery Applet contacts an SNMP agent which has been implemented on the device(s). By sending "get" requests to the SNMP agent via particular addresses within a devices information model called OIDs (Object Identifiers), the requesting software can obtain data values. Only devices that respond affirmatively as being printing devices are queried for data. Only basic information related to printing devices is accessed and collected: Serial number, IP address, Device Make and Model, Page Counts (Total, Color, Copy, Scan, Fax).

Collected information is only forwarded outside of the user's environment when explicitly requested by the user. The Discovery applet uses network bandwidth that is approximately equal to viewing a single website. Scan times will vary depending on amount of network segments designated.

## Application Data Storage

Onsite Database: Oracle 11g

Online Database: SQL 2008