InfoSafe Shredding
Mobile Document Destruction
"Protecting Your Privacy"
402-891-2688

"Protecting Your Privacy"
InfoSafe Shredding
Mobile Document Destruction
(402) 891-2688
www.infosafeshredding.com

FAQ on InfoSafe Shredding Services: Frequently Asked Questions on InfoSafe Shredding
Information And Video on One Time Cleanouts: Cleanouts and Purges

On January 17, 2013 HHS announced a final omnibus rule amending the HIPPA Act of 1996 in accordance with the HITECH Act of 2009. The amendments, which are effective March 26, 2013 supplement and modify the HIPPA Privacy, Security, Breach Reporting and Enforcement Rules. The regulations modify the interim final rule published August 2009 that required notice to patients and others of a "breach" or disclosure of unsecured protected health information (PHI), by covered entities and business associates and their downstream subcontractors.

HIPAA/HITECH Compliance Checklist

There are multiple themes underlying the new rules but this HITECH compliance checklist will focus on the main two.

HITECH Compliance Checklist: Business Associates & Breach Rules

A way to identify the general areas that need addressed for full compliance is to have a **HITECH compliance checklis**t, based on Health & Human Services (HHS) own criteria for an Office of Civil Rights audit with respect these rules. These audits will be conducted every so often and not just in response to complaints. There will be random audits to ensure healthcare organizations and their business associates are in compliance. The compliance audits will touch on the following areas:

1. Policies and procedures
2. Documentation
3. Training and awareness
4. Business associate agreements
5. Attention to security of data and the management thereof

Here is a checklist, based on OCR (Office of Civil Rights) audit procedures for HITECH Compliance

1. HITECH related policies and procedures must be in place, which means having and strengthening user awareness and training. Employees will be asked questions to test their knowledge of HITECH issues during an audit
2. Minimize the capture, storage, & sharing of sensitive information, as the rules and regulations with respect to HITECH focus on securing protected health information. Reducing the different types of interaction with this data means less chance of a breach. Some suggestions here would include moving, as much as possible, your PHI into electronic form (image your paper records), as your ability to control their location and who has access is much greater this way. If you can integrate a document

management system with your data, all the better as this software has very clear audit trails and strong security as far as limiting user roles (access issues), while also allowing you to identify sources of breaches if they occur. Inappropriate use and disclosure of protected health information is the largest cause of complaints. Controlling access and having in place a clear audit trail of who accessed what, when and how they acted on document(s) shows OCR you have done everything possible to protect PHI

3. Ensure your business associates are in full compliance by having HITECH business associate requirements spelled out in a **HITECH business associate agreement**. Then, review these on occasion.
4. Encrypt all identifiable protected health information in both storage and transit contexts. Electronic files can be encrypted and this includes email transfer.
5. As more PHI is passing through mobile devices, implement a security program that targets these devices

HITECH Compliance Checklist – Breach Notification Rules

6. Breach Notification (HITECH 13402) – policies and procedures must be in place and spelt out, in determining when notifications are triggered as a result of breaches.

7. Covered entities much notify individuals
8. Business associates must notify covered entities
9. You have 60 days to complete a notification and no more than that
10. There are different types of notification methods, depending on the number of people whose protected health information was breached
11. The definition of unsecured protected health information is PHI that has not been secured by either encryption and/or destruction. Destruction means the data must be rendered unusable, unreadable, or indecipherable. If PHI has been secured as per HHS guidance (start at page 11, first new paragraph), the notification requirements are not triggered
12. Consider the following as three factors to determine if breach notification is required.

13. was there significant risk of harm to the individual

14. was there inappropriate use or disclosure of unsecured PHI
15. does an exception to the breach rule apply

HITECH Compliance - Security Incidents & Breach Notification

1. Incident reported – log it
2. Did it involve protected health information? Document the incident and conduct breach analysis per above notification requirements
3. As you can see, this involves a lot of documentation. You need a lot in place in policies and procedures as a prevention mechanism. Additionally, if an incident happens, depending on its nature, it may trigger much more documentation with incident reporting and follow up as necessary.