

# **Data Integrity and Data Retention Regulations**

# Increasing Data, Regulations ... and Opportunities

- “In a survey released by the technology company in September, more than half of 158 corporate executives said their businesses have two or three times the amount of information available to them as they had last year.”
- “E-mails, contracts, and PowerPoint files account for 80 percent of corporate information.”
- There are currently over 10,000 U.S. federal, state, and local laws and regulations addressing what, how, when and why records must be created, stored, accessed, maintained, and retained over increasingly longer periods of time
- Many of these mandates carry stiff penalties, including fines and imprisonment
- As a result, companies in all industries are now scrambling to gain “compliance”
- The continuous increase in data, along with the increasing regulations on this data, creates huge opportunities in data storage, backup, and archival solutions



# Regulations Defined: Sarbanes-Oxley Act

- **Sarbanes-Oxley Act**

- Signed into law July 30 2002
- A direct result of corporate scandals, such as Enron and WorldCom
- Introduced legislative changes to financial and corporate regulations
- Intended to "deter and punish corporate and accounting fraud and corruption, ensure justice for wrongdoers, and protect the interests of workers and shareholders" (Quote: President Bush)
- Section 802, Regulation S-X, Rule 2-06
  - All audit and review-related information must be retained for 7 years
  - The penalty for anyone who knowingly destroys documents or files that may relate to a federal investigation or a bankruptcy filing can be fined and/or imprisoned for up to 20 years

# Sarbanes-Oxley Act Penalties

BEHAVIOR	SENTENCE
The alteration, destruction, concealment of any records with the intent of obstructing a federal investigation.	Fine and/or up to 10 years imprisonment.
Failure to maintain audit or review “workpapers” for at least five years.	Fine and/or up to 5 years imprisonment.
Anyone who “knowingly executes, or attempts to execute, a scheme” to defraud a purchaser of securities.	Fine and/or up to 10 years imprisonment.
Any CEO or CFO who “recklessly” violates his or her certification of the company’s financial statements.  If “willfully” violates.	Fine of up to \$1,000,000 and/or up to 10 years imprisonment.  Fine of up to \$5 million and/or up to 20 years imprisonment.
Two or more persons who conspire to commit any offense against or to defraud the U.S. or its agencies.	Fine and/or up to 10 years imprisonment.
Any person who “corruptly” alters, destroys, conceals, etc., any records or documents with the intent of impairing the integrity of the record or document for use in an official proceeding.	Fine and/or up to 20 years imprisonment.
Mail and wire fraud.  Violating applicable Employee Retirement Income Security Act (ERISA) provisions.	Increase from 5 to 20 years imprisonment.  Various lengths depending on violation.

\* Source: Sarbanes-Oxley Act of 2002 and New York City Office of the Comptroller.

# Regulations Defined: HIPAA

## • **Health Insurance Portability and Accountability Act**

- Sets national standards for the healthcare industry
- Addresses the security and privacy of electronic medical-related data, with regard to its use, storage, and exchange
- Section 1173(d)(2)
  - States that reasonable and appropriate administrative, physical, and technical safeguards must be maintained to ensure the integrity of this medical-related data
  - “Data Authentication” - ensuring that data is not altered, destroyed or inappropriately processed
- Medical records must be retained at least 6 years, and at least 2 years after the death of a patient
- Penalties for noncompliance include up to \$250,000 and up to 10 years in prison

# Regulations Defined: Gramm-Leach-Bliley Act

- **Gramm-Leach-Bliley Act**

- Enacted in 1999 by the federal government
- Targeted at the “financial institutions,” including banks, credit unions, collection agencies, credit bureaus, check cashing companies, credit counseling organizations, brokers, tax planning and preparation companies, retailers that issue their own credit cards, auto dealers that lease and/or finance, companies that sell money orders and/or travelers checks, investment companies, investment advisors, and insurance companies
- The Safeguards Rule (16 CFR Part 314): Requires financial institutions to have an administrative, physical, and technical structure to protect the confidentiality and **integrity** of personal consumer information
  - Subtitle A of Title V: Institutions must “protect against any anticipated threats or hazards to the **integrity** of such records”
- Penalties for noncompliance include criminal prosecution, fines, and up to 5 years in prison



# Regulations Defined: SEC 17a-3 and 17a-4

- **SEC regulation 17a-3 and 17a-4**

- Enacted by the SEC in 1997, to allow brokers in the securities industry to store records electronically
- 17a-3: Requirement to make the records
- 17a-4: Requirement to keep the records (retention, WORM non-rewriteable storage, and ease of retrieval)
- In a nutshell, the regulations state that firms must have:
  - Written and enforceable retention policies
  - Storage of data on indelible, non-rewriteable media
  - Searchable index of all stored data
  - Readily retrievable and viewable data
  - Storage of data offsite



# Penalties for Noncompliance: SEC 17a-4

<b>Company</b>	<b>Fine</b>	<b>Violation</b>	<b>Date</b>
<b>SG Cowen</b>	\$100,000	E-mails deleted before retention period expired.	May-03
<b>Deutsche Bank Securities</b>	\$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
<b>Goldman Sachs</b>	\$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
<b>Morgan Stanley</b>	\$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
<b>Salomon Smith Barney</b>	\$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
<b>U.S. Bancorp Piper Jaffray</b>	\$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02



# Regulations Defined: NASD 3010 & 3110

- **NASD 3010 & 3110**

- Rules set by the National Association of Securities Dealers Inc. (NASD)
- Established to govern the behavior of security firms
- Rule 3010: Supervision
  - Each firm must “supervise” their representatives activity, including monitoring incoming and outgoing email
- Rule 3110: Retention of Correspondence
  - Each member shall retain correspondence of registered representatives relating to its investment banking or securities business
  - Requirements pertaining to record keeping formats, mediums, and retention periods comply with SEC Rule 17a-4



# Regulations Defined: NYSE Rule 440

- **NYSE Rule 440**

- Requires brokers and dealers to make and preserve books and records as prescribed by the NYSE and by Rule 17a-3 and Rule 17a-4

# Regulations Defined: SEC 17ad-6 and 17ad-7

- **SEC regulation 17ad-6 and 17ad-7**
  - 17ad-6: What to store and how long...
  - 17ad-7: How to store it...
  - Allows “transfer agents” to use electronic media to maintain their records
    - Transfer Agents: Keep shareholder records, issue new certificates, distribute proxies, dividends and annual reports, and forward company correspondence to shareholders.
  - The rule requires agents to...
    - “Use storage mechanisms that are designed to ensure the accessibility, security, and **integrity** of the records”
    - “Detect attempts to alter or remove the records”
    - “Provide means to recover altered, damaged, or lost records”

# Regulations Defined: 21 CFR Part 11

- **21 CFR Part 11**

- Issued in 1997 by the US Food and Drug Administration (FDA)
- Established standards for electronic information and signatures to replace hard copies for all manufacturers regulated by the FDA
- Requires that “copies” of all records are kept “in common portable formats” and “must preserve the original content and meaning of the records”
- Requires the protection of records to enable their accurate and ready retrieval throughout the records retention period
- Record Retention Periods:
  - Food (Manufacturing, Processing, Packing) – 2 Years After Release
  - Drugs (Manufacturing, Processing, Packing) – 3 Years After Distribution
  - Bio Products (Manufacturing, Processing, Packing) – 5 Years After End of Manufacturing



# Regulations Defined: 17 CFR Part 1

- **17 CFR Part 1**

- Issued in 1999 by the US Commodity Futures Trading Commission (CFTC)
- Amendment to the record keeping requirements of Commission Regulation 1.31
- Allows record keepers to store information either on electronic media or on micrographic media
- Requires that “record keepers store required records on either micrographic or electronic storage media for the full five-year maintenance period”
- “Record keepers will have the flexibility necessary to maximize the cost reduction and time savings available from improved storage technology while continuing to provide Commission auditors and investigators with timely access to a reliable system of records”



# Regulations Defined: FERC Part 125

- **FERC Part 125**

- Regulation of the Federal Energy Regulatory Commission (FERC) under the Federal Power Act and Natural Gas Act
- Sets specific retention periods for the public utilities industry
- Requires the “protection for records...from fire, floods, and other hazards”
- The type of storage media is not specified, however it must have a life expectancy equal to or greater than the specified retention periods



# Regulations Defined: Rev Proc 97-22

## • **Rev Proc 97-22**

- “Guidance on Electronic Records” sets guidelines for record retention and storage recommendations for any and all taxpayers
- States that all “tax related documents” must be retained for as long as they are subject to audit by the IRS under section 1.6001- 1(e)
- The storage system used must:
  - Ensure the integrity, accuracy, and reliability, and
  - Prevent alteration of, deletion of, or deterioration of such records
- Penalties for Noncompliance:
  - The District Director may issue a Notice of Inadequate Records pursuant to section 1.6001-1(d) if the taxpayer's electronic storage system fails to meet the requirements of this revenue procedure.
  - May also be subject to applicable penalties under subtitle F of the Code, including the section 6662(a) accuracy-related civil penalty and the section 7203 willful failure criminal penalty.

# Regulations Defined: NARA Part 1234

- **NARA Part 1234**

- §1234.22 Creation and Use of Text Documents

- Electronic record keeping systems that maintain the official file copy of documents on electronic media must meet the following minimum requirements:

- Provide a method for all authorized users of the system to retrieve desired documents, such as an indexing or text search system;
- Provide an appropriate level of security to ensure **integrity** of the documents (§1234.28-Provides for backup and recovery of records to protect against information loss);
- Provide a standard interchange format when necessary to permit the exchange of documents on electronic media between agency computers; and
- Provide for the disposition of the documents including, when necessary, the requirements for transferring permanent records to NARA



# Regulations Defined: NARA GRS

- **General Records Schedule**

- Issued by the U.S. National Archives and Records Administration (NARA)
- Provides retention schedule for all agencies of the U.S. Federal Government

# Regulations Defined: U.S. Government

- **Dod 5015.2**

- Department of Defense Records Management Program
- Provides mandatory standards for electronic record management systems for the U.S. Department of Defense
- Requirements are based on current NARA regulations
- System Management Requirements
  - C2.2.9.1. Backup of Stored Records. The system must provide the capability to automatically create backup or redundant copies of the records and their metadata
  - C2.2.9.2. Storage of Backup Copies. The method used to back up database files must provide copies of the records and their metadata that can be stored off-line and at separate location(s) to safeguard against loss due to system failure, operator error, natural disaster, or willful destruction.

# Retention Schedule: Financial/Securities

## Financial/Securities

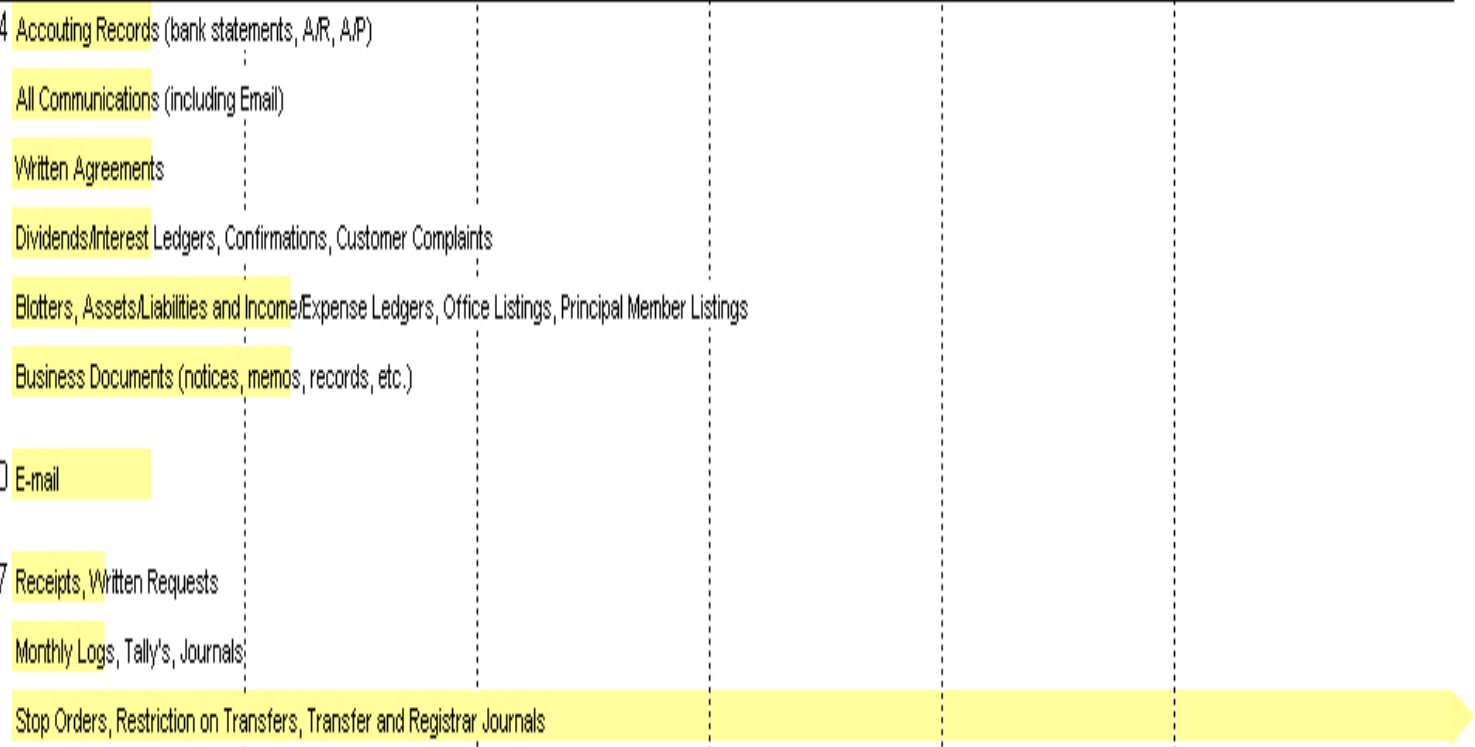
SEC regulation 17a-4 Accounting Records (bank statements, A/R, A/P)  
 All Communications (including Email)  
 Written Agreements  
 Dividends/Interest Ledgers, Confirmations, Customer Complaints  
 Blotters, Assets/Liabilities and Income/Expense Ledgers, Office Listings, Principal Member Listings  
 Business Documents (notices, memos, records, etc.)

NASD 3110 E-mail

SEC regulation 17ad-7 Receipts, Written Requests  
 Monthly Logs, Tally's, Journals

17 CFR Part 1 Trading Cards and Written Customer Orders

Retention Period - Years 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30



# Retention Schedule: Corporate

## Corporate

Rev Proc 97-22 Canceled Checks, Paid Invoices

Bank Statements, Personal Investment Records

Tax Returns, Real Estate Records, Contracts, Leases, and Audit Reports

29 U.S. Code Hiring Documents

Complaints of handicap discrimination

Welfare and Pension plan records

Occupational injuries and illness

Summaries of employee benefit or pension plans

29 CFR 516.2-516.6, 516.11-29 Wages, Hours, Sex, Occupation, Conditions of Employment

8 USC Part 1324a INS Forms

IRS (26 CFR 31.6001) Employment tax records (Social Security documents)

Sarbanes-Oxley Act Audit and Financial Review-Related Information

OSHA Records Related to Employee Exposure to Toxic Substances and Harmful Agents

15 USC Part 2607 Consumer allegations of injury or harm to health

Retention Period - Years 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

# Retention Schedule: Utilities, Manuf., Healthcare

## Public Utilities

FERC Part 125 Annual Reports

Procurement Agreements

General Accounting Ledgers

Plant Ledgers

## Manufacturing

21 CFR Part 11 Food Manufacturing, Processing, Packing Records

Drugs Manufacturing, Processing, Packing Records

Bio Products Manufacturing, Processing, Packing Records

## Healthcare

HIPAA Medical Records after a Patient Death

Adult Medical Records

Pediatric Medical Records

42 CFR Medicare Hospitals: Records on each inpatient and outpatient, records of radiologic service, nuclear medicine including records for the receipt and disposition of radiopharmaceuticals

Comprehensive outpatient rehabilitation facilities (CORFs) under the Medicare program: Clinical records to justify the diagnosis and treatment plan

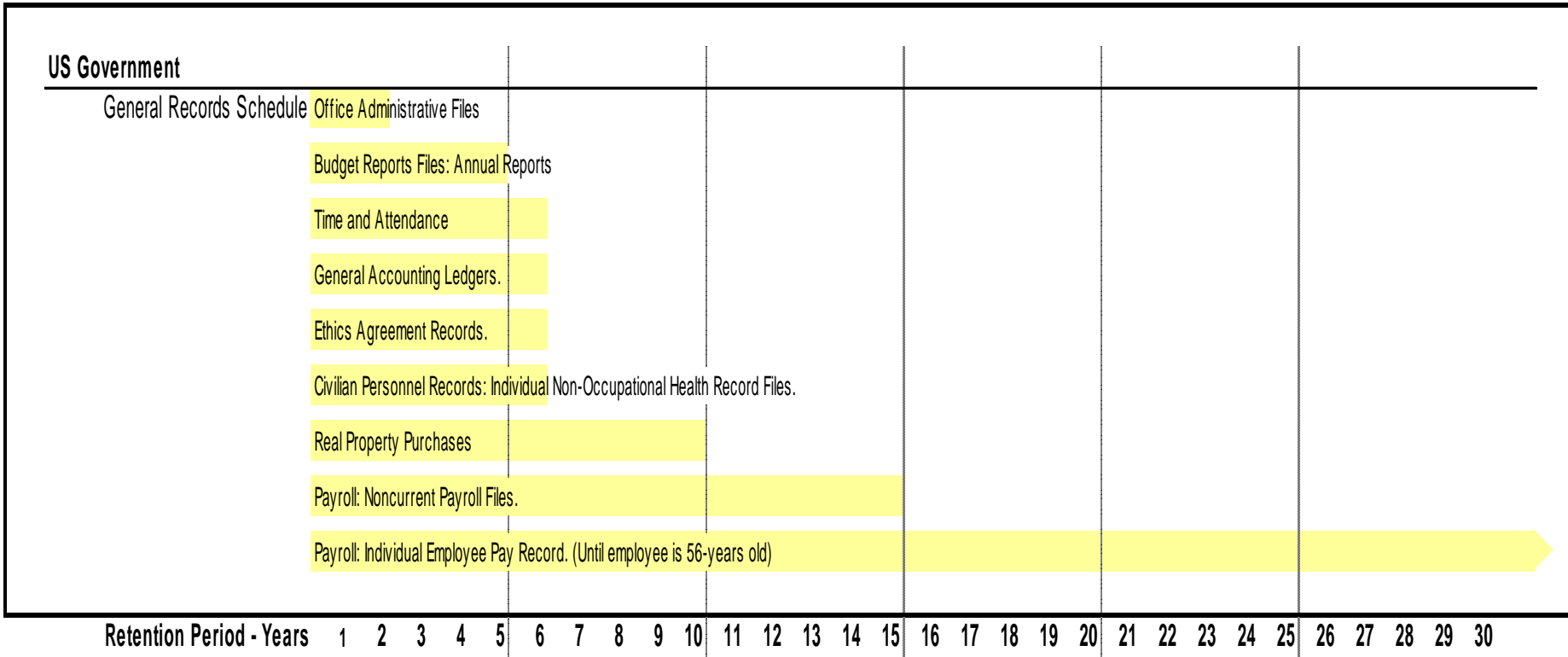
Nursing facilities must retain records for clinical records

Medicare Rural Health Clinics: Medical Records

Retention Period - Years

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

# Retention Schedule: Government



# Thank You

---

## Questions?