





ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES

DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four (4) sensitivity levels:

- **Restricted** 
- **Confidential** 
- **Internal Use** 
- **Public** 

Classification		Data Sensitivity Description
Restricted	Definition	Restricted information is highly-valuable, highly-sensitive business information and the level of protection is dictated externally by legal and / or contractual requirements. Restricted information must be limited to only authorized employees, contractors and business partners with a specific business need.
	Potential Impact of Loss	<ul style="list-style-type: none"> · SIGNIFICANT DAMAGE would occur if Restricted information were to become available to unauthorized parties either internal or external to Forsyth County Schools. · Impact could include negatively affecting Forsyth County Schools competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements and posing an identity theft risk.
Confidential	Definition	Confidential information is highly-valuable, sensitive business information and the level of protection is dictated internally by FCS.
	Potential Impact of Loss	<ul style="list-style-type: none"> · MODERATE DAMAGE would occur if Confidential information were to become available to unauthorized parties either internal or external to Forsyth County Schools. · Impact could include negatively affecting FCS competitive position, damaging the company's reputation, violating contractual requirements and exposing the geographic location of individuals.
Internal Use	Definition	Internal Use information is information originated or owned by Forsyth County Schools or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	<ul style="list-style-type: none"> · MINIMAL or NO DAMAGE would occur if Internal Use information were to become available to unauthorized parties either internal or external to Forsyth County Schools. · Impact could include damaging the company's reputation and violating contractual requirements.
Public	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.

	Potential Impact of Loss	<ul style="list-style-type: none"> · NO DAMAGE would occur if Public information were to become available to parties either internal or external to Forsyth County Schools. · Impact would not be damaging or a risk to business operations.
--	---	--

LABELING

Labeling is the practice of marking a system or document with its appropriate sensitivity level so that others know how to appropriately handle the information. There are several methods for labeling information assets.

- **Printed.** Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page (see below), or simply the words if the graphic is not technically feasible. The exception for labeling is with marketing material since marketing material is primarily developed for public release.
- **Displayed.** CUI-Restricted, Restricted or Confidential information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

GENERAL ASSUMPTIONS

- Any information created or received by Forsyth County Schools employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as “Internal Use” at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential information, the entire application is Confidential.
- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

PERSONAL DATA (PD)

PD is any information about an individual maintained by Forsyth County Schools including any information that:

- Can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and
- Is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Sensitive PD (sPD) is always PD, but PD is not always sPD. Examples of PD include, but are not limited to:

- Name
 - Full name;
 - Maiden name;
 - Mother’s maiden name; and
 - Alias(es);
- Personal Identification Numbers
 - Social Security Number (SSN);
 - Passport number;

- Driver's license number;
- Taxpayer Identification Number (TIN), and
- Financial account or credit card number;
- Address Information
 - Home address; and
 - Personal email address;
- Personal Characteristics
 - Photographic image (especially of the face or other identifying characteristics, such as scars or tattoos);
 - Fingerprints;
 - Handwriting, and
 - Other biometric data:
 - Retina scan;
 - Voice signature; and
 - Facial geometry; and
- Linkable Information
 - Date of birth;
 - Place of birth
 - Race;
 - Religion;
 - Weight;
 - Social / recreational activities or hobbies;
 - Geographical indicators (e.g., geolocation information);
 - Employment information;
 - Medical information;
 - System-specific information (e.g., MAC or hardware address);
 - IP address;
 - Username;
 - Education information; and
 - Financial information.

SENSITIVE PERSONAL DATA (sPD)

Sensitive Personal Data (sPD) is defined as the first name or first initial and last name, in combination with any one or more of the following data elements:

- Government-Issued Identification Number (e.g., passport, permanent resident card, etc.)
 - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
 - Passport number
 - Permanent resident card
- Driver License (DL)
- Financial account number
 - Payment card number (credit or debit)
 - Bank account number
- Electronic Protected Health Information (ePHI)

DATA HANDLING GUIDELINES

Note: For U.S. Government regulated data, the following requirements supersede Forsyth County Schools data handling guidelines:

- For **Federal Contract Information (FCI)**, the following sources are authoritative for FCI data handling:
 - 48 CFR § 52.204-21 (basic safeguarding for Covered Contractor Information Systems (CCIS))
- For **Controlled Unclassified Information (CUI)**, the following sources are authoritative for CUI data handling:
 - 32 CFR § 2002
 - DoD Instruction 5200.48
 - NIST SP 800-171 rev2

Handling Controls	Restricted	Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	<ul style="list-style-type: none"> ▪ NDA is required prior to access by non- employees. 	<ul style="list-style-type: none"> ▪ NDA is recommended prior to access by non-employees. 	<i>No NDA requirements</i>	<i>No NDA requirements</i>
Internal Network Transmission (wired & wireless)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<ul style="list-style-type: none"> ▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<i>No special requirements</i>	<i>No special requirements</i>
External Network Transmission (wired & wireless)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and multi-factor authentication 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<ul style="list-style-type: none"> ▪ Encryption is recommended 	<i>No special requirements</i>

Data At Rest (file servers, databases, archives, etc.)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups 	<ul style="list-style-type: none"> ▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups 	<ul style="list-style-type: none"> ▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups 	<ul style="list-style-type: none"> ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Remote wipe must be enabled, if possible 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Remote wipe must be enabled, if possible 	<ul style="list-style-type: none"> ▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible 	<i>No special requirements</i>
Email (with and without attachments)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Do not forward 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Do not forward 	<ul style="list-style-type: none"> ▪ Encryption is recommended 	<i>No special requirements</i>
Physical Mail	<ul style="list-style-type: none"> ▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper-resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally 	<ul style="list-style-type: none"> ▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper-resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail 	<ul style="list-style-type: none"> ▪ Mail with company interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings 	<i>No special requirements</i>
Printer	<ul style="list-style-type: none"> ▪ Verify destination printer ▪ Attend printer while printing 	<ul style="list-style-type: none"> ▪ Verify destination printer ▪ Attend printer while printing 	<ul style="list-style-type: none"> ▪ Verify destination printer ▪ Retrieve printed material without delay 	<i>No special requirements</i>

<p>Web Sites</p>	<ul style="list-style-type: none"> ▪ Posting to intranet sites is prohibited unless it is pre-approved to contain Restricted data. ▪ Posting to Internet sites is prohibited unless it is pre-approved to contain Restricted data. 	<ul style="list-style-type: none"> ▪ Posting to publicly-accessible Internet sites is prohibited. 	<ul style="list-style-type: none"> ▪ Posting to publicly-accessible Internet sites is prohibited 	<p><i>No special requirements</i></p>
<p>Telephone</p>	<ul style="list-style-type: none"> ▪ Confirm participants on the call line ▪ Ensure private location 	<ul style="list-style-type: none"> ▪ Confirm participants on the call line ▪ Ensure private location 	<p><i>No special requirements</i></p>	<p><i>No special requirements</i></p>
<p>Video / Web Conference Call</p>	<ul style="list-style-type: none"> ▪ Only use secure meeting / videoconference technology ▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location 	<ul style="list-style-type: none"> ▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location 	<ul style="list-style-type: none"> ▪ Pre-approve roster of attendees ▪ Confirm participants on the call line 	<p><i>No special requirements</i></p>
<p>Fax</p>	<ul style="list-style-type: none"> ▪ Attend sending / receiving fax machine to control transmitted material ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval 	<ul style="list-style-type: none"> ▪ Attend sending / receiving fax machine to control transmitted material ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval 	<p><i>No special requirements</i></p>	<p><i>No special requirements</i></p>

Paper, Film/Video, Microfiche	<ul style="list-style-type: none"> ▪ Return to owner for destruction ▪ Owner personally verifies destruction 	<ul style="list-style-type: none"> ▪ Shred or delete all documents or place in secure receptacle for future shredding 	<ul style="list-style-type: none"> ▪ Shred or delete all documents or place in secure receptacle for future shredding 	<i>No special requirements</i>
Storage Media (Hard Disk Drives (HDDs), Flash drives, tapes, CDs/DVDs, etc.)	<ul style="list-style-type: none"> ▪ Physically destroy the hard drives and media ▪ Requires use of company-approved vendor for destruction 	<ul style="list-style-type: none"> ▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient) 	<ul style="list-style-type: none"> ▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient) 	<ul style="list-style-type: none"> ▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient)

K12 LEGAL & REGULATORY ENVIRONMENT

Based on a review of existing K12 data security and compliance requirements, the following laws are applied to educational institutions:

Regulation or Requirement	Description	Required Controls
FERPA (Family Educational Rights and Privacy Act)	Grants access to educational records by parents and eligible students.	N/A
HIPAA (Health Insurance Portability and Accountability Act)	Establishes patient right to privacy from unauthorized disclosure by healthcare facilities and covered entities.	Security Rule – See HIPAA table in section X.X for both <i>required controls</i> and <i>addressable controls</i> (tailorable).
COPPA (Children’s Online Privacy Protection Act)	Applies to websites and online services that collect information from children under the age of thirteen.	N/A
CIPA (Children’s Internet Protection Act)	To address concerns about children's access to obscene or harmful content over the Internet, CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries.	Internet Content Filtering

HIPAA CONTROLS

ADMINISTRATIVE SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	§ 164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	§ 164.308(a)(2)		
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	§ 164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	§ 164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	§ 164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	§ 164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	§ 164.308(a)(8)		
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement	(R)

PHYSICAL SECURITY SAFEGUARDS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	§ 164.310(b)		
Workstation Security	§ 164.310(c)		
Device and Media Controls	§ 164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

TECHNICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	§ 164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	§ 164.312(b)		
Integrity	§ 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	§ 164.312(d)		
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

ORGANIZATIONAL REQUIREMENTS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	§ 164.314(b)(1)	Implementation Specifications	(R)

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
-----------	----------	---	--

Policies and Procedures	§ 164.316(a)		
Documentation	§ 164.316(b)(1)	Time Limit	(R)
		Availability	(R)
		Updates	(R)

STANDARD § 164.312(a)(1) ACCESS CONTROL

“Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)[Information Access Management].”

A covered entity can comply with this standard through a combination of access control methods and technical controls. There are a variety of access control methods and technical controls that are available within most information systems. *The Security Rule does not identify a specific type of access control method or technology to implement.*

UNIQUE USER IDENTIFICATION (R) - § 164.312(a)(2)(i)

The Unique User Identification implementation specification states that a covered entity must assign a unique name and/or number for identifying and tracking user identity.

EMERGENCY ACCESS PROCEDURE (R) - § 164.312(a)(2)(ii)

This implementation specification requires a covered entity to establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

AUTOMATIC LOGOFF (A) - § 164.312(a)(2)(iii)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

ENCRYPTION AND DECRYPTION (A) - § 164.312(a)(2)(iv)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement a mechanism to encrypt and decrypt electronic protected health information.

STANDARD § 164.312(b) AUDIT CONTROLS

The Audit Controls standard requires a covered entity to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

It is important to point out that *the Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed.* A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use EPHI.

STANDARD § 164.312(c)(1) INTEGRITY

The Integrity standard requires a covered entity to implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”

MECHANISM TO AUTHENTICATE ELECTRONIC PROTECTED HEALTH INFORMATION (A) - § 164.312(c)(2)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

STANDARD § 164.312(d) PERSON OR ENTITY AUTHNETICATION

The Person or Entity Authentication standard has no implementation specifications. This standard requires a covered entity to implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

STANDARD § 164.312(e)(1) TRANSMISSION SECURITY

This standard requires a covered entity to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

INTEGRITY CONTROLS (A) - § 164.312(e)(2)(i)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

ENCRYPTION (A) - § 164.312(e)(2)(ii)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

The Security Rule allows covered entities the flexibility to determine when, with whom, and what method of encryption to use. A covered entity should discuss reasonable and appropriate security measures for the encryption of EPHI during transmission over electronic communications networks with its IT professionals, vendors, business associates, and trading partners.

Source: <https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>

ANNEX 2: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

Data Class	Sensitive Data Elements	Public	Internal Use	Confidential	Restricted	CUI - Restricted
Student & Employee Personal Data	Social Security Number (SSN)				X	
	Employer Identification Number (EIN)				X	
	Driver's License (DL) Number				X	
	Financial Account Number				X	
	Payment Card Number (credit or debit)				X	
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)				X	
	Controlled Unclassified Information (CUI)					X
	Birth Date			X		
	First & Last Name		X			
	Age		X			
	Phone and/or Fax Number		X			
	Home Address		X			
	Gender		X			
	Ethnicity		X			
	Email Address		X			
Employee-Related Data	Compensation & Benefits Data				X	
	Medical Data				X	
	Workers Compensation Claim Data				X	
	Education Data			X		
	Dependent or Beneficiary Data			X		
Public Relations & Marketing	Business Plan (including marketing strategy)			X		
Data	Financial Data Related to Revenue Generation			X		
	Marketing Promotions Development		X			
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)	X				
	News Releases	X				
Networking & Infrastructure Data	Username & Password Pairs				X	
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X	
	Hardware or Software Tokens (multifactor authentication)				X	
	System Configuration Settings			X		
	Regulatory Compliance Data			X		

	Internal IP Addresses			X		
	Privileged Account Usernames			X		
	Service Provider Account Numbers			X		
Strategic Financial Data	Corporate Tax Return Information			X		
	Legal Billings			X		
	Budget-Related Data			X		
	Unannounced Merger and Acquisition Information			X		
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X		
Operating	Electronic Payment Information (Wire Payment / ACH)			X		
Financial Data	Paychecks			X		
	Incentives or Bonuses (amounts or percentages)			X		
	Stock Dividend Information			X		
	Bank Account Information			X		
	Investment-Related Activity			X		
	Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)			X		
	Debt Amount Information			X		
	SEC Disclosure Information			X		