

# HEALTH INFORMATION SECURITY

From the Provider's Perspective

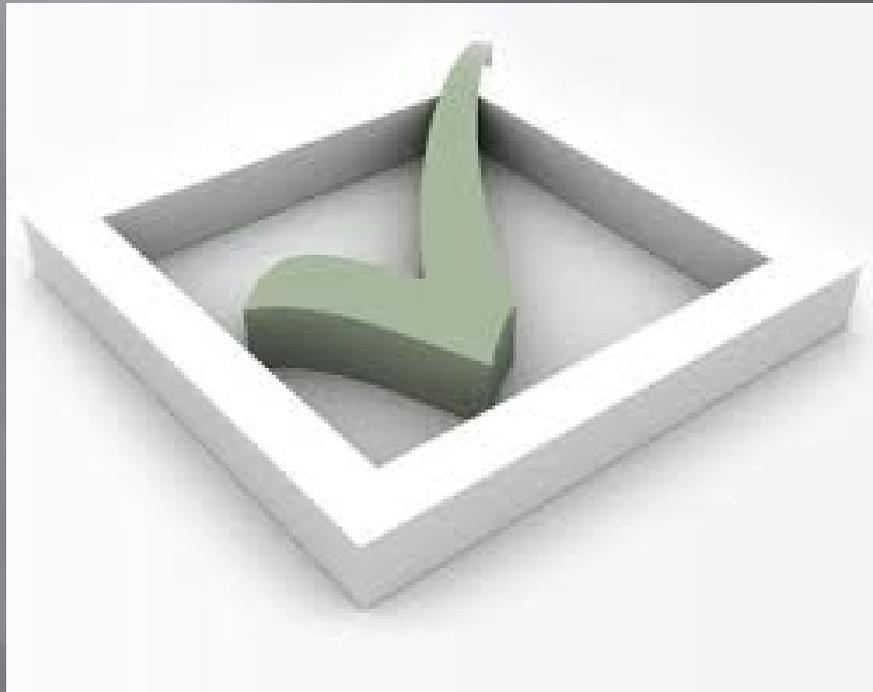
# Protecting PHI



# REGULATIONS



# Compliance



# Compliance

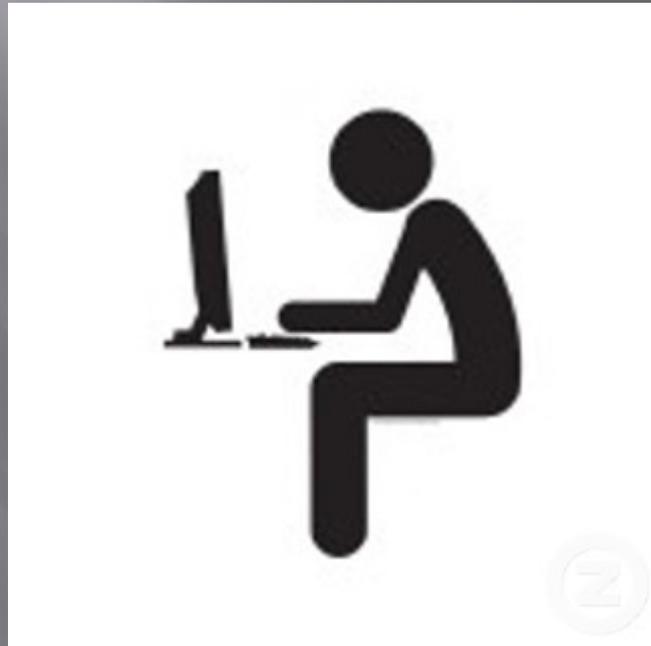
## How to achieve?



# Policies and Procedures



# Agency staff



# Training & Education



Recurring policy & procedure training

Computer training

AKAIMS training



# Physical Access

Access codes



Motion  
cameras



Access cards

ACCESS  
REPORTS

# Clinical offices

Viewable  
Screen  
Unlocked  
office



Auto  
Screen  
lock

AKAIMS  
time-out

# Fax/Copy/Scan/Print

AKAIMS  
notes printed  
and copied

FAX  
confirmation  
pages

Secure print  
option

FAX cover  
sheets

Secure  
scan  
folders

Hard drive  
retention



# Laptops

Contain  
PHI?

Do they  
leave  
the  
office?

Wireless  
access?

Hard drive  
encryption



# Voicemail

Confidential  
messages



User  
PIN

Speaker  
off for  
voicemail

# Clinical sessions

Office  
conversation  
overheard in  
hallways



Provide  
whitenoise

# Reception area

Receptionist  
conversations

Files on  
counters

Viewable  
screens

Glass  
windows

Locking  
windows

Screen  
orientation  
and auto  
lock



# Passwords

Simple

Never changed

Written down

Forgotten

Shared

Stolen  
electronically

Social  
engineering

Virus/intrusion  
protection

Training

Monitoring

Lockout

Memorize



# Virus & Intrusion Prevention

Automatically  
updated

Centrally  
monitored

Layered



# Email

PHI in email

Encrypted

AeHN Secure  
Messaging

Policies for PHI  
docs from email



# Clinical supervision

Recordings

Storage &  
Encryption

Access control



# Data Leak Protection

Securing  
endpoints

Electronic tagging  
of sensitive data



# Remote access

AKAIMS access

Policies and  
Monitoring

Access control



# Provider AKAIMS help desk

Provider help desk  
responsibilities

Password resets

Permissions changes

24/7 operations



# Skills

Keyboarding

Navigation

Browsing



# Policy Matrix

## Quick Reference

	LABEL NAME			
	Public	Internal	Confidential	Restricted Confidential
<ul style="list-style-type: none"> <li>• <b>Email within the organization</b></li> </ul>	No special handling required	No special handling required	Use of client name prohibited, unless encrypted or emergency situation. Use of email strongly discouraged. Broadcast to distribution lists is prohibited.	Use of any client identifier prohibited. Use of email strongly discouraged, unless emergency situation. Notify recipient in advance. Broadcast to distribution lists is prohibited.
<ul style="list-style-type: none"> <li>• <b>Email outside of the organization</b></li> </ul>	No special handling required	No special handling required	Use of client name prohibited, unless encrypted or emergency situation. Use of email strongly discouraged. Broadcast to distribution lists is prohibited.	Use of any client identifier prohibited. Use of email strongly discouraged, unless encrypted or emergency situation. Notify recipient in advance. Broadcast to distribution lists is prohibited.
<ul style="list-style-type: none"> <li>• <b>FAX – Location of fax machine</b></li> </ul>	Located in area not accessible to public	Located in area not accessible to public	Located in area not accessible to public	Located in area not accessible to public and unauthorized persons.
<ul style="list-style-type: none"> <li>• <b>FAX – Use of fax coversheet</b></li> </ul>	Required	Required	Required. Cover sheet labeled Confidential. No client identifiers on cover sheet	Required. Cover sheet labeled Restricted Confidential. No client identifiers on cover sheet
<ul style="list-style-type: none"> <li>• <b>Fax – Transmission Safeguards</b></li> </ul>	Reasonable care in dialing	Reasonable care in dialing	Procedures to validate transmission to intended recipient, e.g. validated direct dial key, confirmation print out.	Telephone notification prior to transmission and subsequent telephone confirmation of receipt required.