

Wedgwood Christian Services



HIPAA

The Health Insurance Portability
and Accountability Act of 1996
(Section II)

What Does HIPAA Cover?



Transactions, Privacy, and Security of Protected Health Information (“PHI”)

- PHI is individually identifiable health information
- What is considered identifiable information?
- Permitted disclosures/access/use of PHI:
 - Treatment
 - Payment (billing)
 - Internal Operations-agency management, clinical supervision, QI, COA, licensing, audits, etc)

Most Significant Changes



Required Staff Appointments: “Privacy Officer”, “Contact Person”, and “Security Officer”

- Privacy Officer takes overall responsibility for Privacy systems
- Contact Person manages day-by-day activities of client privacy systems
- Security Officer
- Revised/New Policies, Revision Of Existing Forms (consent, release) approximately 14 New Forms

Most Significant Changes



“Notice of Privacy Practices”

- A statement of how a person’s PHI is kept confidential, secure, and is disclosed
- Must give to all current clients by 4/14/03
- (mailing or at their first contact after that date)
- Must give to all new clients starting 4/14/03
- (included in the admissions procedures)

Clients Must Acknowledge Receipt of Notice

- There’s a form for this; clerical will be trained and have the form available.

Most Significant Changes



Client May Refuse to Sign Acknowledgment

- There's a form for this; clerical will be trained and have the form available.

Client May Request Restrictions on Use of PHI that is outlined in the "Notice of Privacy Practices"

- There's a form for this; clerical will be trained and have the form available. We do not have to honor request for restrictions.

Most Significant Changes



New Privacy and Information System Policies

- To be approved by the Board on 4/22/03

Staff Acknowledgment Form (Signed by Staff)

- Acknowledges receipt of policies
- Acknowledges responsibility to follow policies
- Staff includes foster parents, volunteers, students, and teachers (not divulging of educational records but WW records/PHI of a client)

HRD Policy- must include consequences of violation

Business Associate Agreements - all those who perform a function on the agency's behalf (vendors)

Most Significant Changes



Acknowledgements, Consents and Authorizations - What's the Difference?

- **Acknowledgement** – signed acknowledgement of a client that they have read and understand our privacy practices.
- **Consent** – signed permission of a client to use their PHI for reasons allowed by HIPAA-treatment, payment or operations.
- **Authorization** – signed permission of a client to share their PHI with entities outside of our need for treatment, payment or operations.

Most Significant Changes



“Persons of Least Privilege” access restrictions

Tracking Disclosures

- No longer simply maintaining a copy of the release requests; a new form that will be maintained by clerical that logs in each file all authorized disclosures

Disposal of Records

- Greater need for assurance that the records are, in fact, destroyed – a more robust document destruction procedure that is pending

Most Significant Changes



Internal Handling of Client's PHI

(*Written* Records **and** *Oral* Communication)

- Always sign in/sign out of a client record (closed also)
- Never to be taken off agency premises (certain exceptions will exist, and procedures for these will be developed - e.g., for court hearings)
- Never left unattended or overnight on desks
- Always locked up in overhead, locked office if not in file
- Never left open on computer screens

Most Significant Changes



Internal Handling of Client's PHI

continued

(*Written Records and Oral Communication*)

- Never left at unattended fax machines
- Never visible to non-Wedgwood employees when accessed via dial-in access from home computers
- Always destroyed from home computer files
- Never used in internal or external emails
- Never used in greetings in public areas/places

Most Significant Changes



- **Disaster Recovery/Business Continuity Plans**
- **Reporting breaches of security**
- **Visitor sign in/out, badges, escorts - all sites**
- **Unique Situations**
 - Disclosure to family and friends when client is unable
 - Disclosure in cases of emergency
 - Revocation of a consent
 - Amendments to the client record
 - Right to review and copy their record
 - Right to an accounting of disclosures

Rights of Clients



For all of the following client situations, a form is available from clerical staff and consultation is available through the Client Rights Advisors:

To Revoke a Consent or Authorization

- *Clients have the right to change their mind and no longer permit us to use their information for treatment, payment or operations*

To Review and Get a Copy of their Record

- *Clients have the right to see what's in their file and get a copy of it.*

Rights of Clients



To Amend a Record

- *Clients have the right to add something to the file if they believe it is important to do so.*

To Request Confidential Communications

- *Clients have the right to request that we handle our communications with them in a special way; we do not have to honor the request.*

To Complain About our Privacy Practices

- *Clients have the right to complain about our Privacy Policies, Practices, or compliance with the state/federal laws regarding them.*

Rights of Clients



To **Request Restrictions on Use** of Their PHI For Treatment/Payment/Operations

- *Clients have the right to request that we not use their PHI in some way that it is legal for us to use it; we do not have to honor it.*

To an **Accounting of Disclosures** (Non-TPO)

- *Clients have the right to have an accounting made of any disclosures that have been made from their file to anyone not covered by the Treatment, Payment, Operations exceptions.*

Information Systems



- Applicable to Everyone!
- Computers are for Agency Business
- Computer Information
 - Must safeguard like paper records
 - Privacy Policies and Procedures still apply
 - Wedgwood business information applicable too
 - If information is not required for you to do your job, you are not permitted to access it (“persons of least privilege” restricted access)

Information Systems



Use of Wedgwood Information Systems

- Authentication of User Identity
 - Users must keep your ID Confidential!
 - Each person will have a User ID - it is confidential and may not be shared with others
 - When Users log onto our computer system, they will be asked to enter a User Identity.

Information Systems



Use of Wedgwood Information Systems

- Passwords and Password Management
 - New Passwords
 - at least 6 characters in length
 - mix of letters and numbers
 - avoid use of words, names of family members or pets, sports teams or other obvious passwords
 - no “password” passwords
 - Keep passwords confidential!
 - Don't keep written passwords in obvious places
 - Change every ninety days (and no alternating!)

Information Systems



Use of Wedgwood Information Systems

- Automatic Logoff - 30 Minutes
- Access Control
 - ID/Password permission-based on work performed and records needed to perform job
- Workstation Use
 - Official software only; changes only with the permission of the Information Systems staff

Information Systems



Use of Wedgwood Information Systems

- Virus Protection
 - All computers will have virus protection; all home computers used for work must have it as well
- Firewalls
 - All computers will have software to prevent unauthorized access; all home computers too
- Report Procedures
 - Security breaches - must be reported to Information System staff immediately

Information Systems



Use of Wedgwood Information Systems

- Disposal of Electronic Media
 - If you keep confidential Wedgwood business information or protected health information on any electronic media (includes portable computers, home computers, PDA's, floppy disks, CD-R's, CD-RW's, tapes or other electronic media), notify an Information System staff. The storage devices of any such electronic media must be specially "cleaned" or physically destroyed

Information Systems



Use of Wedgwood Information Systems

- Equipment Control
 - Sign-out any computer equipment you wish to remove from Wedgwood's premises
 - Register any computer equipment that is brought onto Wedgwood's premises
- Electronic Mail
 - Obligation to use email appropriately, effectively, and efficiently; greater awareness and discretion needed with email than with other documents!
 - can be intercepted
 - can be printed
 - can be forwarded
 - can be stored by others

Information Systems



Use of Wedgwood Information Systems

- Electronic Mail
 - Email messages may not include information that could be used to identify an individual as a client, or any information about their health or wellbeing
 - Email messages that include sensitive information should include a subject header or “flag” to indicate that the communication is personal and confidential

Information Systems



Use of Wedgwood Information Systems

- Electronic Mail
 - Messages in Wedgwood's email system are Wedgwood's property
 - Users have no guarantee of privacy relating to their use of Wedgwood's e-mail system
 - Wedgwood may access the email system to read any user's email to ensure that it is being used for legitimate business purposes

Information Systems



Use of Wedgwood Information Systems

- Electronic Mail
 - Email messages are temporary communications, non-vital and may be discarded routinely
 - Email messages important to the treatment of an individual client or the operation of Wedgwood's business should be retained in accordance with practices that apply to paper records
 - Any email pertaining to a Wedgwood client should be filed in the individual's electronic or paper record

Information Systems



Use of Wedgwood Information Systems

- Electronic Mail
 - May use email to communicate with clients; however, must inform them that:
 - Email is not appropriate for emergencies
 - Email is not appropriate for time-sensitive issues
 - Email should not be used for highly sensitive or personal information unless it is the communication is encrypted
 - Email that contains PHI from Wedgwood will be encrypted

Information Systems



Use of Wedgwood Information Systems

- Electronic Mail

- May use email to communicate with clients; however, must inform them that:

- Staff other than a clinician may read or process the email
- No one can guarantee security or privacy
- Any email message from them should include (1) the type of message in the subject line (e.g. appointment request, request for call, etc.), and (2) clear client identification including client name and contact information in the body of the message

Use of Information Systems



Internet Access

- Users may access the Internet through Wedgwood's network. Except for incidental personal use (non-work interfering), access to the Internet should be for Wedgwood business purposes only. Users should not access the Internet using dial-up modems, except as authorized by the System Administrator.

Use of Information Systems



Remote Access Policy

- Wedgwood will allow a limited number of Users the right to access the computer system from remote locations. Remote access rights must be approved by the Executive Director (or designee).
- In order to ensure the security of our computer system and safeguard confidential information, the following policies apply:
- Dial-up modems must be configured to provide secure network access

Use of Information Systems



Remote Access Policy

- Access to Wedgwood's internal network from outside of the network must be controlled by a secure means (e.g., Citrix qualifies); Information Systems staff will work with authorized Users to set up remote access
- Persons authorized to work at home or otherwise have remote access to Wedgwood's computer system must install anti-virus software and intrusion detection software on computers used for those purposes

Use of Information Systems



Prohibited Uses of Wedgwood Computer System

- Copying or transmission of any document, software or other intellectual property protected by copyright, patent or trademark law, without proper authorization by the owner of the intellectual property
- Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing

Use of Information Systems



Prohibited Uses of Wedgwood Computer System

- Political activities including sending political messages and solicitation of funds
- Gambling
- Viewing, downloading, or exchanging pornography
- Illegal activities of any kind
- Disclosure of protected health information in a manner inconsistent with our Privacy Policies and Procedures

Use of Information Systems



Prohibited Uses of Wedgwood Computer System

- Use of e-mail addresses for marketing purposes without explicit permission from the target recipient
- Forwarding of e-mail from in-house or outside legal counsel, or the contents of that mail, to individuals outside of the company without the express authorization of counsel
- Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication

Use of Information Systems



Prohibited Uses of Wedgwood Computer System

- Obtaining access to the files or communications of others with no substantial company business purpose
- Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization

Use of Information Systems



Enforcement

- Employees of Wedgwood who violate any part of this policy are subject to disciplinary action up to and including dismissal
- Wedgwood reserves the right to immediately terminate for cause any contract or business relationship with any User who violates any part of this policy
- Wedgwood will report to appropriate authorities any violation of this policy that is a violation of the law

Wedgwood Christian Services



**Thank You for
Participating in
this Training!**