goodweek

DATA BREACH POLICY

V2.0

The owner of the policy is David Masson, CLO

goodweek

VERSION	STAKEHOLDER	NAME	DATE	CONTENT
1.0	Author	V. Laffite	11/07/2025	Initial version
	Validation	D. Masson	11/10/2025	
2.0	Author	V. Laffite	09/01/2026	Annex for HIPAA Breach Procedures for Protected Health Information (PHI)
	Validation	D. Masson	09/07/2026	

PROPRIETARY & CONFIDENTIAL

goodweek

1. Purpose

This policy sets out how Goodweek responds to data and cyber breaches. It applies in situations where there is an actual, potential or suspected data breach.

2. Data Breach Response

What is a data breach?

A data breach for this purpose of this policy occurs where there is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, **confidential data or personal data** transmitted, stored or otherwise processed.

Examples of a breach involving loss of personal data could include where

- a device containing a copy of Goodweek's client database is stolen or lost
- an encryption key for a particular data set is no longer in its possession
- data is deleted by an unauthorized individual
- there is significant disruption to the normal service of Goodweek and personal data is temporarily or permanently unavailable
- It could also involve malware, intrusion attempts, theft of equipment, software corruption, human error and unauthorized access attempts

What should you do if you think a personal Data Breach has occurred?

If you become aware of any circumstances in which you suspect that a data breach may have occurred or is likely to occur, you must act immediately and notify the Chief Legal Officer (CLO) and the management. This should be treated as a priority. Your notification to the CLO and the management should be made by email marked "high importance" and the subject line should state "Data Breach", using the address: **privacy@goodweek.com**

You should ensure you follow your email with a phone call to ensure the email has been read and acted upon. The following information should be included within your email to the extent you know them:

(a) details of the actual, potential or suspected breach and how it occurred or may occur
(b) if a data breach has occurred, the time and date that the breach occurred and was discovered and whether the incident is continuing
(c) names of offices (if applicable) affected
(d) the categories of data breached or the data that is likely or suspected to be breached
(e) the approximate number of personal data records affected by the breach (if known)
(f) the approximate number of individuals affected by the breach (if known)

(g) the IT systems / Platform / equipment involved
(h) the location of the equipment and the names and contact details of any individual involved, if known
(i) the likely consequences / repercussions of the data breach (for example identity fraud, relevant Goodweek's Client(s), damage to reputation of the individual or financial loss)
(j) the measures taken or proposed to be taken to address the breach or potential or suspected breach, including, where appropriate, measures to mitigate its possible consequences

In no circumstances should you delay reporting the breach simply because you do not have all this information. Further information can be provided in phases provided it is done so without undue delay.

Investigation

The CLO will inform the Head of Engineering who will make an initial determination of whether or not there has been a data breach, discussing the facts with relevant personnel and make a preliminary determination of the risk to the individuals concerned.
If the determination is that there may have been a data breach causing risk to individuals, the CLO will notify relevant stakeholders and the C-levels of the data breach and coordinate an investigation. Depending on the personal data involved, the relevant stakeholders could be the CEO, Head of Engineering, COO and lead HR.
The investigation should include responses to the following questions:

(a) When did the breach occur and when were we made aware?
(b) What is the nature of the breach and how did it occur? (For example, theft or unauthorized access etc.)
(c) What is the source of the breach?
(d) What categories and numbers of (i) individuals; and (ii) data records are subject to the breach?
(e) What are the likely consequences of the breach? Consider identity theft or fraud, financial loss, discrimination, damage to the reputation of the individual, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization and any other significant economic or social disadvantage.
(f) What is the severity of the potential impact of the breach on the individuals concerned?
(g) What steps can be and have been put in place to mitigate the impact and stop any further breaches?
(h) Who is aware of the breach internally and/or externally?

Irrespective of whether a decision is taken to report the breach, the CLO should ensure a written record of this investigation is maintained. The Supervisory Authority may require a copy of this report as part of their investigation into any reported security breach or to assess compliance with legislative requirements.

Mitigation

The CLO should identify and implement steps to ensure the breach is contained and to mitigate and manage its impact. The CLO will consult the DPO in case of personal data at stake.

Report to the Supervisory Authority/ies

Where Goodweek is the data controller, and in accordance with the recommendation of the General Counsel, Goodweek must notify the relevant data breach to the supervisory authority as soon as it becomes aware of the breach, unless it can demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of individuals.

There are only limited circumstances when such risk can be eliminated, for example: the data disclosed by a breach are public; the data are encrypted and backed up and the key is not compromised or capable of being ascertained by technical means available to unauthorized persons; the data are securely hashed and salted, and the key used to hash the data was not compromised in any breach and the key used was generated such that it could not be ascertained by technical means available to unauthorized persons.

Goodweek should ensure that the company reports the data breach to the Supervisory Authority without undue delay and in any event **within 72 hours** of becoming aware of the data breach. This notice should contain the following information:

(a) the nature of the data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned

(b) the name and contact details of the CLO (DPO if personal Data) or other contact point where more information can be obtained

(c) the likely consequences of the data breach

(d) the measures taken or proposed to be taken by the controller to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In no circumstances should the DPO delay reporting the data breach simply because he does not have all this information. Further information can be provided in phases provided it is done so without undue delay.
After making an initial notification, the Goodweek/DPO will be able to update the Supervisory Authority/ies if a follow-up investigation uncovers evidence that the security incident was contained, and no breach actually occurred. This information can be added to the information already given to the Supervisory Authority/ies and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

If the data breach relates to personal data for which Goodweek is a processor, Goodweek shall notify the data controller without undue delay.

Notification to Individuals

When Goodweek is a controller of the affected data, and according to the CLO's assessment, Goodweek should notify the individuals affected or potentially affected if the data breach is likely to result in a high risk to their rights and freedoms. Examples of where notification should be made include where the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality of data protected by professional security or any other significant economic or social disadvantage.

Any notification should be made without undue delay in clear language and include the following information:
(a) the name and contact details of the DPO or other contact point where more information can be obtained
(b) the nature of the data breach
(c) the likely consequences of the personal data breach
(d) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, recommendations of ways for the individual to mitigate the adverse effects of the data breach such as resetting of passwords or other access credentials.

A notification to an individual affected by the data breach will not be necessary if in the following conditions:

(a) Goodweek has implemented appropriate technical and organizational protection measures, such as encryption, to ensure that the personal data subject to the breach is unintelligible to any person who is not authorized to access it

(b) Goodweek has taken measures to ensure the data breach will not result in a high risk to the rights and freedoms of individuals

(c) it would involve disproportionate effort, in which circumstances, a public communication or similar could be made

However, please note that the Supervisory Authority may still require that Goodweek notify the relevant individuals.

Record Keeping

Goodweek's team under supervision of CLO, shall keep and maintain the documentation of all personal data breaches, including all minutes and decisions taken during the investigation of any actual, potential or suspected breach.

goodweek

Appendix - HIPAA Breach Procedures for Protected Health Information (PHI)

Procedures

In the event that Goodweek identifies a potential breach of **PHI occurs**, the following procedures shall be followed.

Step 1: Identification (Discovery)

A breach of PHI will be deemed "discovered" as of the first day Goodweek knows of the breach or, by exercising reasonable diligence, would or should have known about the breach.
If a potential breach is discovered, it is very time sensitive and must be immediately reported.

The following is full description of what constitutes PHI:
PHI is any health information that can be tied to an individual to include the following:

1. Names (Full or last name and initial)
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers (including serial numbers and license plate numbers)
13. Device identifiers and serial numbers
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

There are also additional standards and criteria to protect individual's privacy from reidentification. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed.
For example, a subject's initials cannot be used to code their data because the initials are derived from their

name. Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study.
In other words, the information would still be considered identifiable if there was a way to identify the individual even though all of the 18 identifiers were removed.

Step 2: Initial Reporting / Escalation

If there is belief that a potential breach of PHI has occurred, **the CTO & COO or their designated representative, must be immediately notified.**

Please provide all of the information available at the time of the initial regarding the potential breach, to include the following:

- Names
- Dates
- The nature of the PHI potentially breached
- The manner of the disclosure (fax, email, mail, verbal)
- All employees involved
- The recipient
- All other persons with knowledge
- Any associated written or electronic documentation that may exist.

Notification and associated documentation may itself contain PHI and should only be given to the designated Security Officer, or their designated representative.
Do not discuss the potential breach with anyone else, and do not attempt to conduct an investigation as these tasks will be performed by the designated Security Officer, or their designated representative.

Step 3: Investigation

Upon receipt of notification of a potential breach the designated CTO, or their designated representative shall promptly conduct an investigation.
The investigation shall include the following activities:

- Interviewing employees involved
- Collecting written documentation
- Completing all appropriate documentation
- Forensic investigation (optional depending on incident)

The CTO or designated representative, shall retain all documentation related to potential breach investigations, in accordance with established record retention requirements, or for a minimum of six years, whichever is greater.

Step 4: Risk Assessment and Recommendation

Upon completion of the investigation, the CTO & COO shall perform a Risk Assessment to determine if the use or disclosure of PHI constitutes a breach and requires further notification to the Covered Entity.

The designated CTO & COO shall appropriately document the Risk Assessment and make a recommendation to executive management regarding whether notification to the Covered Entity of the potential breach would be prudent.

When executing the risk assessment, a “reasoned judgment” standard will be applied to the incident which shall be fact specific, and shall include consideration of the following factors:

- Did the disclosure involve Unsecured PHI in the first place?
- Who impermissibly used or disclosed the Unsecured PHI?
- To whom was the information impermissibly disclosed?
- Was it returned before it could have been accessed for an improper purpose?
- What type of Unsecured PHI is involved and in what quantity?
- Was the disclosure made for any improper purpose?
- Is there the potential for significant risk of financial, reputational, or other harm to the individual whose PHI was disclosed?
- Was immediate action taken to mitigate any potential harm?
- Do any of the specific breach exceptions apply?

Step 5: Final Determination

Goodweek's executive management in collaboration with legal counsel shall, after review of the evidence and risk assessment, have final authority to determine whether a breach of PHI occurred and what, if any, further action is warranted.

Step 6: Notification

In the event that Goodweek's executive management and/or legal counsel determines that notice to the Covered Entity or Business Associate is warranted, Goodweek's executive management and/or legal counsel or the designated representative shall promptly prepare and transmit a notice to the Covered Entity.

Timing of Notification

Goodweek shall notify the Covered Entity "without unreasonable delay" but no later than **60 days after discovery and/or notification of the breach,** as required by law.

Goodweek Service and Business Associate Agreements provides that Goodweek is an independent contractor; therefore, the Covered Entity's time to provide the requisite notice begins to run on the date that Goodweek notifies the Covered Entity of the breach1.

Delay of Notification

1. Unjustified Delay

If it appears to the CTO that the investigation will not be completed within a reasonable time, executive management and/or legal counsel shall be informed to ensure that the Covered Entity will be notified before completion of the investigation.

2. Law Enforcement Delay

A delay in notification is permissible if a law enforcement official states that a breach notification would impede a criminal investigation or cause damage to national security

If a law enforcement request is received, the law enforcement statement must be in writing and must specify the length of the delay required.

If the request for a delay in notification is oral, Goodweek must document the statement and request written confirmation within 30 days. If no written request for a delay is received within that time, Goodweek must send notification of the breach to the Covered Entity.

[1] Verify and modify language as needed to ensure consistency with customer contracts and BAAs

Content of Notification
Any notification to the Covered Entity (CE) provided by Goodweek shall include all information as required by law, but at a minimum, will contain the following content:

- Identification of each individual whose PHI is believed to have been breached
- The date of the incident discovery
- The date of disclosure
- The facts and circumstances surrounding the disclosure
- All associated documentation
- All other available information known to Goodweek that the Covered Entity will be required to include in its own Notice to the individual(s).
- Any additional information regarding the breach that Goodweek discovers after the initial notice to the Covered Entity be promptly provided to the Covered Entity as required by law.
- Any notice to the Covered Entity shall be sent via first class mail with a return receipt requested and the return receipt as well as a copy of the Covered Entity Notice shall be kept with related documentation and retained in accordance with established record retention requirements or for a minimum of six years, whichever is greater.

Step 7: Documentation

All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate that all appropriate steps were completed. All supporting documentation associated with the potential breach shall be kept on file in accordance with established record retention requirements or for a minimum of six years, whichever is greater.

Internal HIPAA Breach Checklist

- Following any actual or suspected breach of unsecured electronic protected health information (ePHI), Goodweek must notify the affected Covered Entity (CE) or Business Associate.
- **Notify the CTO and Legal of a suspected ePHI breach, within four (4) hours.**
- Incident Response Team investigates suspected breach and execute risk assessment to verify if ePHI data has been compromised.
- Incident Response Team shall complete a Breach Notification Report
- Incident Response Team provides the completed Breach Notification Report to the Security Officer for review and approval
- The CTO review and approve the submitted Breach Notification Report
- The CTO provides a copy of the final Breach Notification Report to Goodweek Legal department within one (1) business day after approval
- Legal reviews Breach Notification Report and submits the report to the Covered Entity through approved communication channels
- Legal will ensure that notification to the Covered Entity occurs no later than sixty (60) calendar days following the initial discovery of a breach or suspected breach, unless delayed by an appropriate law enforcement agency.

HIPAA Breach Notification Content and Template

- The Breach Notification Report to the Covered Entity (CE) notification must include the following information.
- Identification of each individual associated with the affected Covered Entity (CE) whose ePHI was

suspected to have been accessed, acquired, used, or disclosed (to the extent possible).

- Any other information that the covered entity is required to include in notification to the affected individual under CFR 164.404(c) which includes:
- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
- Any steps individuals should take to protect themselves from potential harm resulting from the breach.

goodweek

HIPAA Breach Notification Template

Information Security: HIPAA / ePHI Breach Notification Report	
Incident Number: <###-MMYYYY or Ticket #>	
Other Incidents Related to this Incident:	
Breach Incident Status	(i.e., New, In progress, Forwarded for investigation, Resolved)
Incident Summary	Description of what happened and is known to date
Incident Description	Date and Time Incident Discovered:
	Date and Time Incident Reported:
	Date and Time Incident Occurred:
	Place of Incident:
	Personnel Involved in Incident:
	Type and Volume of Information Involved:
	Accessibility/Vulnerability of ePHI / Protective Controls in Place: (e.g. Encryption, etc.):
	Indicators of Compromise Related to the Incident:
	Root Cause of Incident:
	Awareness of Incident (who knows about it now):
Initial Risk Assessment	Number of Individuals Potentially Affected:
	Potential Privacy Breach (Yes/No):
	Risk to Individuals (Types and Extents):
	Financial Risk to Organization:
	Legal/Contractual Risk to Organization:
	Regulatory Risk to Organization:
	Public Relations Risk to Organization:
	ePHI Accessed or Modified in an Unauthorized Manner (Yes / No):
Steps Taken	Current Actions Taken:
	Evidence Gathered / Chain of Custody:
	People Contacted: (e.g., system owners, system administrators, Law enforcement, outside counsel, forensics investigators):
	Data Breach Services Provider Contacted:
	Agencies Notified:
	Close or Move to Investigation Phase and Why:
Notification	Covered Entity(s) (CE) Affected:
	Date Covered Entity(s) (CE) Notified:
	Method(s) used to Notify Covered Entity(s) (CE):
	Notification Record (Ticket # Documenting Notification):
	System Generated List of Individuals Affected Attached (Required):

	Supporting Details:
Recommendations	Immediate Notification Requirements: Affected Covered Entities MUST be notified within sixty (60) days of a suspected breach.
	Priorities and Considerations for Further Investigation
	Next Steps to be Taken (e.g., Rebuild the host, upgrade an application, implement additional controls, etc.).
	Recommendations for Affected Individuals:

HIPAA - HHS/OCR Investigations and Records Availability Procedure

1. Purpose

Goodweek maintains a process to make its policies, procedures, and records available to the U.S. Department of Health and Human Services ("HHS"), including the Office for Civil Rights ("OCR"), when required for an investigation or determination of compliance with applicable HIPAA requirements.

2. Scope

This procedure applies to all Goodweek personnel and to any request from HHS, OCR, or another authorized governmental authority concerning HIPAA compliance, privacy, security, breach notification, or records availability.

3. Receipt and Escalation of Requests

Any employee who receives a request, inquiry, subpoena, audit notice, or other communication from HHS, OCR, or another governmental authority related to HIPAA must promptly forward it to the CLO and COO.

The CLO or COO will:

- Log the request in the compliance request register;
- Verify the authenticity, scope, and deadline of the request;
- Notify relevant internal stakeholders;
- Coordinate the collection and review of responsive information; and
- Maintain a record of all communications and materials provided.

4. Availability of Policies, Procedures, and Records

Goodweek will make relevant policies, procedures, documentation, and records available to HHS/OCR as required by applicable law and within the requested or legally required timeframe.

Responsive records may include, as applicable:

- HIPAA privacy, security, and breach notification policies and procedures;
- Risk analyses and risk management documentation;

- Workforce training records;
- Business Associate Agreements and related contractual documentation;
- Incident, breach, and complaint records;
- Audit logs, access-control records, and security documentation; and
- Other records relevant to the investigation or compliance determination.

Before disclosure, Goodweek will review the requested materials to ensure that the response is complete, accurate, appropriately scoped, and transmitted through a secure method.

5. Cooperation as a Business Associate

When Goodweek acts as a Business Associate, it will cooperate with the applicable Covered Entity in responding to requests from HHS/OCR concerning services performed on the Covered Entity's behalf.

If Goodweek receives an individual request for access to, amendment of, or accounting of disclosures of Protected Health Information ("PHI") on behalf of a Covered Entity, Goodweek will document the request and promptly forward it to the applicable Covered Entity, unless otherwise required by law or expressly permitted or required by the applicable Business Associate Agreement.

Goodweek will provide reasonable assistance to the Covered Entity, consistent with the applicable Business Associate Agreement, to enable the Covered Entity to meet its HIPAA obligations.

6. Documentation and Record Retention

Goodweek will retain documentation related to HHS/OCR inquiries and responses, including:

- The original request or notice;
- Internal review and decision records;
- Communications with HHS/OCR, the applicable Covered Entity, and legal counsel, where applicable;
- Copies of documents and records provided; and
- Evidence of the method and date of transmission.

Documentation will be retained in accordance with Goodweek's record-retention requirements and applicable HIPAA retention obligations.