

Integrated Dermatology, LLC HIPAA Privacy Policies

CC-P-001	Affiliated Covered Entity
CC-P-002	Authorization for Use of Disclosure of PHI
CC-P-003	Privacy Officer
CC-P-004	Permitted Uses and Disclosures of PHI
CC-P-005	PHI Enforcement Safeguard Mitigation Discipline
CC-P-006	Minimum Necessary Standard
CC-P-007	Notice of Privacy Practices
CC-P-008	Faxing PHI
CC-P-009	Verification of Identity and Authority Before Disclosing PHI
CC-P-010	Patient Right to Request and Accounting of Disclosure
CC-P-011	Business Associate Policy
CC-P-012	Patients Right to Request an Amendment of PHI
CC-P-013	Privacy Training for Members of the Workforce
CC-P-014	Patients Right to Request Privacy Restrictions
CC-P-015	De-Identifying PHI
CC-P-016	Limited Data Set-Permitted Purposes for Use and Disclosure
CC-P-017	Uses and Disclosures of PHI for Marketing
CC-P-018	Uses and Disclosures of PHI for Which an Authorization is Not Required
CC-P-019	Privacy and Security of Non-Electronic PHI
CC-P-020	Subpoenas and Court Orders
CC-P-021	Uses and Disclosures of PHI for Treatment, Payment, and Healthcare Operations
CC-P-022	Patient's Right to Access PHI
CC-P-023	Complaints and Reporting
CC-P-024	Breach Reporting
CC-P-025	Social Media

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-001
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Designation of Integrated Dermatology Covered Entities as an Affiliated Covered Entity ¹ ("ACE")
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Policy Purpose:

The Health Insurance Portability and Accountability Act of 1996, as modified by the Health Information Technology for Economic and Clinical Health Act (collectively, "HIPAA") sets forth certain organizational requirements under 45 CFR §164.105. Under 45 CFR §164.105(b), two (2) or more separate legal entities under common ownership or control may designate themselves as Affiliated Covered Entity ("ACE") for Privacy Rule compliance. The purpose of this policy is to designate certain healthcare components of Integrated Dermatology, LLC as a single ACE

Scope:

This policy applies to all Integrated Dermatology, LLC and the healthcare components of Integrated Dermatology, LLC, designated as an Affiliated Covered Entity, specifically. The healthcare components of Integrated Dermatology, LLC are covered entities² that are under common control³ or under common ownership⁴ of Integrated Dermatology, LLC, as listed in Exhibit A of this Policy.

Policy & Procedure:

1. ACE designation permits sharing of Protected Health Information⁵ ("PHI") among all the covered entity companies of the ACE designation as if they were a single entity. Sharing PHI within the ACE is a use of PHI, and not a disclosure of PHI
2. Under the ACE designation, only one (1) set of HIPAA compliance documents needs to be developed, maintained, and enforced by the ACE:
 - a. HIPAA Privacy and Security Policies
 - b. HIPAA Privacy and Security Officer(s)
 - c. Business Associate Agreements ("BAA")
 - d. Notice of Privacy Practices ("NPP")
 - e. Training of HIPAA Privacy and HIPAA Security
 - f. HIPAA Security Risk Assessment
 - g. HIPAA Patient Authorization Form; and
 - h. Any other compliance documents needed to adhere to HIPAA rules and regulations.

3. An ACE must remain a written or electronic record of a designation. Documentation of this designation of an ACE relationship must be retained for at least six (6) years from the date when it last in effect.

¹An affiliated covered entity ("ACE") refers to legally separate covered entities that are affiliated (under common ownership or control) and designate themselves as a single covered entity for the purposes of complying with HIPAA.

²Covered Entity refers to any health care provider that transmits health information in electronic form in connection with a transaction covered by HIPAA.

³Common Control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

⁴Common Ownership exists if an entity or entities possess an ownership or equity interest of 5% or more of other entity.

⁵Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

Related Forms:

List of Affiliated Covered Entities

Related Policies:

Resources:

45 CFR §105(b)-Affiliated Covered Entities

45 CFR §105(c)-Documentation

List of Affiliated Covered Entities

US Pathology Lab
On-Site Dermatology
Dermatology of Century Village
Integrated Dermatology Group, LLC-Ellicott City (PC)
Integrated Dermatology of 19th Street, LLC
Integrated Dermatology Management LLC (MSO)
Integrated Dermatology of Bluefield, PLLC (PC)
Integrated Dermatology of Boise, LLC
Integrated Dermatology of Boulder Creek, LLC
Integrated Dermatology of Bountiful, LLC
Integrated Dermatology of Bridgeport, PLLC (PC)
Integrated Dermatology of Brookline, LLC (PC)
Integrated Dermatology of Chesterfield, LLC
Integrated Dermatology of Clinton, LLC (PC)
Integrated Dermatology of Columbus, LLC
Integrated Dermatology of Enfield, LLC
Integrated Dermatology of Fairfax, LLC
Integrated Dermatology of Florida, LLC-Boca Raton (PC)
Integrated Dermatology of Glades Road, LLC
Integrated Dermatology of Gloucester, LLC
Integrated Dermatology of Granville, LLC
Integrated Dermatology of Groton, LLC
Integrated Dermatology of I Street, LLC
Integrated Dermatology of K Street, LLC
Integrated Dermatology of Lakeport, PC
Integrated Dermatology of Lincoln, PC (PC)
Integrated Dermatology Management of CA, LLC
Integrated Dermatology of Louisiana II, LLC-Ponchatoula (PC)
Integrated Dermatology of Mass Ave, LLC
Integrated Dermatology of Massachusetts, LLC-Quincy (PC)
Integrated Dermatology of Mississippi, LLC-Greenville (PC)
Integrated Dermatology of Montrose, LLC
Integrated Dermatology of New Jersey, LLC-East Brunswick (PC)
Integrated Dermatology of North Raleigh, PLLC (PC)
Integrated Dermatology of Northshore, LLC
Integrated Dermatology of Reno-Mortensen, PLLC
Aistheta Reno Medical Skin Care Center

Integrated Dermatology of Reston, LLC
Integrated Dermatology of Roseville, PC (PC)
Integrated Dermatology Management of California, LLC (MSO)
Integrated Dermatology of S. Burlington, PLLC (PC)
Integrated Dermatology of S. Miami, LLC
Integrated Dermatology of Sanford, PLLC
Integrated Dermatology of Santa Rosa, PC (PC)
Integrated Dermatology of Silver City, LLC
Integrated Dermatology of Sunset Drive, LLC (PC)
Integrated Dermatology of Tidewater, LLC
Integrated Dermatology of Vernon, PLLC (PC)
Integrated Dermatology of Waterbury, LLC (PC)
Integrated Dermatology of Westlake Village (PC)
Integrated Dermatology of White Plains, LLC (PC)
Integrated Dermatology of Worcester II, LLC (PC)
Integrated Dermatology of Yuma, LLC
Latham Dermatology, PLLC (PC)
ID Management of New York, LLC (MSO)
Salida Dermatology
Summit Plastic Surgery & Dermatology, PLLC (PC)
Westminster Dermatology, LLC

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-002
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Authorization ¹ for Use ² or Disclosure ³ of Protected Health Information ("PHI") ⁴
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce⁵, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG

IDG must obtain a HIPAA compliance Authorization for Release of Information Form that is completed and signed by the patient or his/her legal representative before using or disclosing the individuals' health information for purposes other than treatment⁶, payment⁷, and health care operations⁸, or other disclosures permitted without an authorization.

Policy & Procedure:

4. If an individual presents an Authorization form other than the IDG form, review the form first to ensure all the required elements are included and addressed. The form must contain the following required elements and must be written in plain language.

Valid Authorization Requirements

- i. The form must be signed by the patient or legal/personal representative not more than sixty (60) days before presented to IDG.
- j. The patient's signature and date are on the authorization, if a personal representative of the individual signs the authorization, a description of such representative's authority to act for the individual must also be provided.
- k. Include sufficient specific information for the patient to be accurately identified.
- l. Specify to whom the information is to be sent (full name and complete address).
- m. State the reason for the request and disclosure.
- n. A description of the PHI to be used or disclosed that identifies the information in a specific, meaningful fashion.
- o. IDG must be listed as the releasing entity

- p. An expiration date or event that relates the patient or the purpose of the disclosure.
 - q. A statement that the provision of treatment and payment may not be conditioned on obtaining this authorization.
 - r. A statement of the individual's right to revoke the authorization in writing, how to invoke the right to revoke and exceptions to this right.
 - s. Any consequences that will result from the patient's refusal to sign (including a statement that treatment cannot be conditioned on signature and any exceptions that might apply).
 - t. A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure and no longer protected by HIPAA.
 - u. For authorizations related to marketing, any remuneration that the covered entity⁹ might be receiving.
5. A IDG Authorization for Release of Information is available on ADP under HIPAA Privacy Policies.
6. An authorization is not valid if the:
- a. Authorization does not include the elements noted in section 1 of this policy.
 - b. Expiration date has passed.
 - c. Expiration even is known by IDG to have occurred.
 - d. Information in the authorization is known by IDG to be false.
 - e. Authorization has been inappropriately combined with another document.
4. Revocation of Authorization
- a. A patient may revoke an authorization at any time.
 - b. The revocation must be in writing.
 - c. IDG honors the revocation upon receipt; however, the revocation does not affect uses or disclosures made by IDG prior to its receipt of the revocation.
5. Authorization is not required for the following:
- a. Disclosures for treatment, payment, or healthcare operation.
 - b. Disclosures required by state or federal law.
 - c. Disclosures to public health agencies and health oversight agencies.
 - d. Disclosures to authorities for abuse, neglect, and domestic violence.
 - e. Disclosures for judicial and administrative proceedings.
 - f. Disclosures for certain law enforcement purposes.
 - g. Disclosures to coroners, funeral director, or medical examiners.
 - h. Disclosures to organ donation procurement agencies.
 - i. Disclosures for workers compensation.
 - j. Disclosures to avert serious threats to public health or safety

¹An authorization means a detailed document that gives IDG permission to use PHI for specified purposes, which are generally other than treatment, payment, and healthcare operations, or to disclose PHI to a third party specified by the individual

²Use means sharing, employing, applying, utilizing, examining, or analyzing PHI within IDG

³Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG

⁴Protected Health Information (“PHI”) contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

⁵Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

⁶Treatment means the provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination or management of healthcare by a healthcare provider with a third party; consultation between healthcare providers relating to a patient; or the referral of a patient for healthcare from one healthcare provider to another

⁷Payment means activities undertaken by IDG to obtain payment or reimbursement for the provision of healthcare by IDG

⁸Healthcare Operations means services or activities that are necessary (and to the extent necessary) for IDG to carry out its functions as a healthcare provider

⁹Covered Entity refers to any healthcare provider that transmits health information in electronic form in connection with a transaction covered by HIPAA

Related Forms:

Authorization for Release of Information

Related Policies:

Patient’s Rights to Access Health Information-CC-P-022

Marketing Uses and Disclosures-CC-P-017

Resources:

45 CFR §164.508-Uses and disclosures for which an authorization is required

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-003
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Privacy Officer
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC (“IDG”), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce¹, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG

The IDG Privacy Officer is a designated employee who develops, implements, and manages IDGs policies and procedures regarding the privacy of protected health information (“PHI”)². The Privacy Officer works to keep IDG in compliance with applicable federal and state laws; receives privacy complaints; manages IDGs privacy education programs; and provides guidance to workforce members on IDG privacy practices and policies.

Policy & Procedure:

1. The IDG Privacy Officer has the following general responsibilities:
 - a. Developing, implementing, and managing IDG policies and procedures regarding the privacy of PHI in compliance with applicable federal and state laws.
 - b. Receiving IDG privacy complaints and ensuring appropriate investigations and resolution of such complaints.
 - c. Receiving workforce members privacy complaints and ensuring appropriate investigation and resolution of such complaints.
 - d. Answer questions related to IDG’s Notice of Privacy Practice.
 - e. Perform privacy risk assessments and conducting related ongoing compliance monitoring activities.
 - f. Ensure that IDGs workforce members receive appropriate privacy training.
 - g. Overseeing compliance with IDG privacy policies, including sanctions for failing to comply with such policies.
 - h. Reviewing and revising IDG privacy policies, authorization forms, business associate agreement (“BAA”)³, materials, and notices to ensure that IDG is following applicable federal and state requirements.
 - i. Initiating and promoting activities and communication within IDG to foster privacy awareness.

- j. Maintain current knowledge of applicable federal and state laws and regulations and accreditation standards relating to privacy and confidentiality.
 - k. Participate in external privacy compliance reviews or investigations.
-

¹Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

²Protected Health Information (“PHI”) contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

³Business Associate Agreement (“BAA”) means an agreement made between IDG and business associates who have access to PHI.

Related Forms:

Notice of Privacy Practice

Related Policies:

Notice of Privacy Practices-CC-P-007

Patient Privacy Restrictions-CC-P-014

Complaint and Reporting-CC-P-023

Resources:

⁴45 CFR §164.530-Administrative Requirements

**Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-004
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Permitted Uses ¹ and Disclosures ² of Protected Health Information ("PHI") ³
Effective:	11/1/22
Approval:	10/21/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce⁴, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG

Policy & Procedure:

1. IDG workforce members may use or disclose PHI only as described below:
 - a. To the patient, with proper identification and only after viewing a valid authorization.
 - b. To the personal representative of the patient or, with written authorization from the personal representative, as permitted in such authorization.
 - c. For treatment⁵, payment⁶, or healthcare operations⁷.
 - d. For certain uses or disclosures without an authorization as permitted by IDG policy. All such disclosures will be made in a manner consistent with the IDG Notice of Privacy Practice (NPP)⁸.
 - e. To create de-identified health information⁹.
 - f. To a business associate¹⁰, provided the business associate has a written and signed Business Associate Agreement ("BAA")¹¹ with IDG that contains PHI protection. Assurances before the use or disclosure of any PHI as required by policy.
 - g. Uses and disclosures required or permitted by law regarding PHI of a deceased individual.
 - h. Uses and disclosures for research purposes.
 - i. By verifying the identity and authority of the person who is requesting PHI.
 - j. Complying with the policy and procedure governing marking activities involving the use or disclosure of PHI.
 - k. To provide a limited data set¹² to a limited set recipient.
 - l. To individuals involved in patient's care (or for notification purposes).
 - m. Workforce members may use or disclose PHI that has been deidentified

2. IDG must make reasonable attempts to limit the uses or disclosure of PHI to the minimum necessary.
-

¹Use means sharing, employing, applying, utilizing, examining, or analyzing PHI within IDG

²Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG

³Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

⁴Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

⁵Treatment means the provision, coordination, or management of healthcare and related services by IDG

⁶Payment means activities undertaken by IDG to obtain payment or reimbursement for the provisions of healthcare by IDG

⁷Healthcare operation means services or activities that are necessary for IDG to carry out its functions as a healthcare provider.

⁸Notice of Privacy Practice (NPP) is a general description of the patient's rights with respect to PHI, how IDG may use and disclose PHI and IDG's legal duties with respect to PHI.

⁹De-identified is health information that does not identify a patient and which IDG does not reasonably believe can be used to identify a patient.

¹⁰Business Associate means a person or entity that uses or discloses PHI to perform a function or activity on behalf of IDG. A business associate is not a member of the workforce. All business associates must sign a business associate agreement satisfactory to IDG before providing any services to or on behalf of IDG.

¹¹Business Associate Agreement ("BAA") means an agreement made between IDG and business associates who have access to PHI.

¹²Limited Data Set is PHI that excludes the following direct identifiers of the individual or of relatives, employers or household member of the individual: names, postal address information, other than city or town, state and zip code; telephone number; fax numbers; email addresses; Social Security Number; medical record number; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and

serial numbers; URLs; IP addresses; biometric identifiers, including finger and voice prints; and full-face photographic images and any comparable images.

Related Policies:

Authorization for Use and Disclosure of PHI-CC-P-002

Minimum Necessary Requirements-CC-P-006

Notice of Privacy Practices-CC-P-007

Verification and Identity and Authority of PHI-CC-P-009

Business Associates-CC-P-011

De-Identifying PHI-CC-P-015

Limited Data Set-CC-P-016

Uses and Disclosures for Marketing-CC-P-017

Uses and Disclosures for with Authorization is not required-CC-P-018

Uses and Disclosures for Payment, Treatment and Healthcare Operations-CC-P-021

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-005
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Protected Health Information (PHI) ¹ Enforcement: Safeguards ² , Mitigation ³ , and Discipline ⁴
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC (“IDG”), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce⁵, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG maintains appropriate safeguards to ensure the privacy of PHI.

IDG mitigates, to the extent practicable, any harmful effects IDG identifies as having been caused by the inappropriate use of disclosure of PHI.

IDG appropriately disciplines workforce members who fail to comply with IDG policies and procedures regarding use⁶ and disclosure⁷ of PHI.

Policy & Procedure:

1. During new hire orientation and annual mandatory training sessions, workforce members will be made aware of the potential discipline for violating HIPAA policies and procedures for protecting PHI.
2. IDG enforces the appropriate use and disclosure of PHI by:
 - a. Maintaining appropriate administrative, technical, and physical safeguards to ensure the privacy of PHI.
 - b. Appointing a Privacy Officer to coordinate and oversee IDG’s privacy policies and practices.
 - c. Appointing a Security Officer to coordinate and oversee IDG’s information security policies and practices.
 - d. Disciplining workforce members who fail to comply with IDG’s policies and procedures regarding use and disclosure of PHI.
 - e. Mitigation, to the extent practicable, any harmful effects IDG identifies as having been caused by the inappropriate use of disclosure of PHI.

3. The Privacy Officer periodically reviews IDG's HIPAA Privacy policies and procedures and Notice of Privacy Practices (NPP)⁸ and recommends changes or new policies and procedures as appropriate.
4. Any patient of client who feels IDG has inappropriately used, or disclosed PHI may file a complaint.
5. Upon notification of an alleged privacy violation, IDG will take the following steps as Appropriate:
 - a. Investigates the reported violation
 - b. Determines the source of the violation
 - c. Determines the severity and magnitude of the violation
 - d. Determines if the violation is on-going
 - e. Takes action to stop the violation
 - f. Takes action to correct the effects of the violation to the extent possible and/or;
 - g. Communicates the outcome of the investigation to the affected partie(s).
6. If a workforce member uses or disclosed PHI in violation of IDG's HIPAA policies, IDG imposes appropriate discipline, taking into account:
 - a. The severity of the violation
 - b. Whether the violation was accidental or intentional
 - c. Whether the violation was part of a pattern of violations
 - d. IDG's standard disciplinary process.
7. If a business associate⁹ uses or discloses PHI in violation of IDG's HIPAA policies, IDG Takes action which may include, but is not limited to:
 - a. Counseling the business associate regarding the violation
 - b. Reviewing the business associate's HIPAA Privacy program
 - c. Monitoring the business associate's performance to ensure that the wrongful behavior has been remedied; and/or
 - d. Terminating the contract if the violation continues or if the contract cannot be terminated, notifying the Secretary of the Department of Health and Human Services.
8. A workforce member who reports suspected HIPAA violations to IDG thru the hotline or other reporting mechanisms, a governmental agency, accreditation organization, or other agency or body under applicable whistleblower laws or regulations will not be disciplined as long as the report was made in good faith.

¹Protected Health Information (“PHI”) contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

²Safeguard means privacy and information security measures that IDG selects, develops, implements, and maintains to protect PHI and to manage the conduct of approved individuals who interact with PHI.

³Mitigation means minimizing or lessening the effects of an identified PHI privacy violation.

⁴Discipline means penalties IDG imposes for noncompliance with IDG policies and procedures.

⁵Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

⁶Use means sharing, employing, applying, utilizing, examining or analyzing PHI within IDG

⁷Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG

⁸Notice of Privacy Practice (NPP) is a general description of the patient’s rights with respect to PHI, how IDG may use and disclose PHI and IDG’s legal duties with respect to PHI

⁹Business Associate means a person or entity that uses or discloses PHI to perform a function or activity on behalf of IDG. A business associate is not a member of the workforce. All business associates must sign a business associate agreement satisfactory to IDG before providing any services to or on behalf of IDG.

Related Form

Notice of Privacy Practice

Code of Conduct

Related Policies:

Privacy Officer-CC-P-003

Complaint and Reporting Policy-CC-P-023

Breach Notification Policy-CC-P-024

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-006
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Minimum Necessary Standard
Effective:	11/1/22
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce¹, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

Policy & Procedure:

1. Each IDG workforce member must have a legitimate "need to know" prior to accessing using² or disclosing³ protected health information ("PHI")⁴. Each workforce member may only access, use or disclose the minimum amount of PHI necessary to perform his or her designated role, regardless of the extent of access to PHI is provided to him or her.
2. When using, disclosing, or requesting PHI, IDG makes reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purposes of the use, disclosure or request.
3. With respect to system access, IDG complies with the minimum necessary standard by making reasonable efforts to implement authorizations, access (such as role-based access) and/or audit controls for all systems that contain PHI.
 - a. IDG identifies workforce members or categories of workforce members who need access to PHI to carry out their IDG job functions and determines the level of access necessary and any conditions appropriate to the access.
 - b. IDG makes reasonable efforts to limit the access of any workforce member to only those types of PHI necessary for the individual to fulfill his or her job duties.
4. For non-routine disclosures of and requests for PHI, IDG will make every attempt to limit PHI to the amount reasonably necessary to accomplish the purpose of the disclosure or request. Each non-routine disclosure or request is reviewed individually to ensure compliance with the criteria

5. The minimum necessary standard does not apply to:
- a. Disclosures to or requested by a healthcare provider for treatment
 - b. Uses or disclosures made to an individual or personal representative regarding the individual's PHI
 - c. Uses or disclosures made pursuant to an authorization
 - d. Disclosures made to the Secretary of the Department of Health and Human Services
 - e. Uses or disclosures that are required by law; and
 - f. Uses or disclosures that are required for IDG to comply with the HIPAA Privacy and Security Rules.
-

¹Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

²Use means sharing, employing, applying, utilizing, examining, or analyzing PHI within IDG

³Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG

⁴Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

Related Policies:

Permitted Uses/Disclosures of PHI-CC-P-004

Uses and Disclosures of PHI for which an Authorization is Not Needed-CC-P-018

Resources:

45 CFR § 164.502(b)-Minimum Necessary

45 CFR § 164.514(d)-Other requirements relating to uses and disclosures of PHI

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-007
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Notice of Privacy Practice ("NPP") ¹
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce², independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

Policy & Procedure:

1. The NPP is a general description of:
 - a. The patient's rights with respect to protected health information ("PHI")³
 - b. The uses and disclosures of PHI that may be made by IDG
 - c. IDG's legal duties with respect to PHI
2. The NPP contains language that is required by law. The NPP will not be revised without consulting the Compliance Officer, Privacy Officer, Risk Management and Legal Counsel.
3. The NPP will indicate that all complaints will be forwarded to the Privacy Officer or the Secretary of Health and Human Services.
4. If the NPP is revised, IDG must make the revised notice available upon request, post the revised NPP on the public website, and must post it in a clear and prominent location where it is reasonable to expect individuals to see it.
5. IDG reserves the right to change its privacy practices and NPP at any time within the confines of applicable law. Any change IDG makes to its privacy practices and NPP will apply to all PHI maintains.
6. IDG will display the NPP on its Public Website in a clear and visible manner.

¹Notice of Privacy Practice (NPP) is a general description of the patient's rights with respect to PHI, how IDG may use and disclose PHI and IDG's legal duties with respect to PHI.

²Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

³Protected Health Information (“PHI”) contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

Related Forms:

Notice of Privacy Practice

Related Policies:

Privacy Officer PHI-CC-P-003

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-008
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Faxing Protected Health Information ("PHI") ¹
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce², independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG maintains appropriate safeguards to ensure the privacy and security of PHI that is sent or received by facsimile (fax)

IDG takes reasonable steps to manage the privacy risks posed by misdirected faxes and location of equipment sending or receiving faxes in unsecured areas.

Policy & Procedure:

1. This policy applies to all faxes containing PHI that is sent or received by IDG and/or workforce members. At IDG, faxes may be sent or received by a dedicated fax machine, a multi-function printer or a computer-based fax application.
2. Fax machines are useful tools for rapidly and cost-effectively conveying information and documents within IDG and to outside entities with whom IDG does business. However, transmitting PHI by fax may pose privacy risks in the form of misdirected faxes and the delivery to or receipt of faxes in unsecured areas.
3. IDG limits the use³ and disclosure⁴ of and requests for PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
4. IDG limits PHI transmissions to legitimate business purposes such as patient care and treatment, bill and payment matters and appropriate administrative matters necessary to conduct IDG operations.

5. IDG takes reasonable steps to ensure the faxes containing PHI are sent to and received by the intended recipient(s) to protect the privacy and security of the PHI. Reasonable steps may include, but are not limited to, the following:
 - a. Transmitting PHI by fax only when the transmission is time-sensitive and delivery by regular mail or secure electronic transmission will not meet the reasonable needs of the sender or recipient.
 - b. Pre-programming fax machines or software with the fax numbers of frequent PHI recipients to minimize the risk of misdirected faxes associated with manual entry of fax numbers.
 - c. Double-checking fax numbers prior to beginning a transmission when manual entry of a fax number is necessary.
 - d. Using IDG's standard fax cover sheet that contains the necessary confidentiality statement.
 - e. Including the fax recipient's name, business affiliation, telephone number and fax number, as well as the number of pages contained in the transmission, on the fax cover sheet.
 - f. Checking fax confirmation sheets as soon as possible after the fax has been transmitted to confirm that the materials reached the intended recipient. If the intended recipient notifies IDG that the fax was not received, the sender will use their best efforts to determine whether the fax was sent to another number.
 - g. Responding promptly when an individual learns that a fax was sent to an incorrect number by contacting that recipient to request the fax (and any copies) be returned to IDG or shredded and reporting the incident to the individual's supervisor, Privacy Officer, and/or the Compliance Officer to determine if a reportable breach has taken place.

6. IDG takes reasonable steps to ensure that intended recipients of faxes containing PHI are not viewed or received by someone else. Reasonable steps may include, but are not limited to, the following:
 - a. Limiting unauthorized access to fax machines, computers, and printer, such as by placing devices in secure areas that are not accessible to the general public.
 - b. Checking fax machines and printers regularly to minimize the amount of time that incoming faxes containing PHI are left on the machines.
 - c. Delivering incoming faxes to the recipient promptly.
 - d. Notifying the sender of a misdirected incoming fax, or the IDG employee for whom it was intended, and arranging for appropriate delivery, destruction, or return.
 - e. Advising individuals and organizations that frequently send faxes to IDG of changes to the individual's or department's fax number.

¹Protected Health Information (“PHI”) contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

²Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

³Use means sharing, employing, applying, utilizing, examining, or analyzing PHI within IDG

⁴Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG

Related Forms:

IDG Fax Cover Form(s)

Related Policies:

Permitted Uses/Disclosures of PHI-CC-P-004

Minimum Necessary Standard-CC-P-006

Breach Notification-CC-P-024

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-009
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Verification of Identity and Authority before Disclosing Protected Health Information ("PHI") ¹
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce², independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

This policy requires individuals to confirm the identity and authority of unknown persons or entities before disclosing PHI on behalf of IDG.

Policy & Procedure:

1. Prior to disclosing PHI, each individual must confirm that the disclosure is permitted by IDG policy.
2. IDG must verify the identity and authority of every unknown person or entity before disclosing PHI, whether the disclosure occurs in person, orally, or in writing.
3. Identity of Requestor-Prior to disclosing PHI, IDG must verify the identity of any unknown individual or entity through any one of these options listed below:
 - a. Viewing a valid state or federal issued photo ID (driver's license, passport, military identification or state identification card) or:
 - b. Confirming (verbally or in writing) a minimum of three items from the following list of acceptable identifiers:
 1. Patient Social Security Number, or at least last 4 digits (required) and
 2. Patient date of birth (required):
 3. Any one of the following:
 - a. Account number
 - b. Street address
 - c. Insurance Carrier Name
 - d. Insurance Policy Number
 - e. Medical Record Number

- f. Birth Certificate
- g. Insurance Card

4. Authority of Requestor-Prior to disclosing PHI, IDG must verify the authority of any unknown individual or entity, through any of the options listed below. No proof of authority is necessary if the patient (or the parent of a minor parent) is requesting a disclosure of PHI.
 - a. Authorization of the patient
 - b. Signed Durable Power of Attorney for Healthcare
 - c. Guardianship papers if the patient is a minor or has been judged legally incompetent
 - d. Papers issued by a probate court appointing the requestor as executor or administrator of a patient's estate.

5. Third Party Requestors-To verify that a requestor is truly a representative of a third party (such as an insurance company) and that the request is on behalf of the third party, the following information should be taken into consideration when reviewing the request.
 - a. Letterhead: Request is on official printed letterhead and PHI is mailed or faxed to the address or number printed on the letterhead:
 - b. E-mail address: Request is received via email from an email address that identifies the company (example: Jane.Doe@aetna.com)
 - c. Fax coversheet with company logo: Request information is mailed or faxed to address or number listed on the coversheet
 - d. Photo ID: With official credentials when a third-party request is made in person, including a request from a member of law enforcement or a public official
 - e. Telephone ID: Request is made by phone and ID is valid to who is requesting PHI

6. IDG must comply with all other applicable policies before disclosing PHI.

7. IDG may disclose PHI to public officials or someone acting on the official's behalf (such as law enforcement officials) with or without a subpoena under the following circumstances:
- a. The official has presented one or more of the following pieces of identification
 1. Agency identification badge
 2. Other official credentials
 3. Other proof of government status (photo ID issues by gov't agency)
 4. A request written on official government letterhead
 5. A written statement on appropriate gov't letterhead that the person Making the request is acting under the government's authority (example: a nonprofit company hired by a county health department To compile statistics on meningitis cases).
 - b. The individual follows the procedures outlined in the Subpoenas and Court Order policy.
-

¹Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

²Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

³Use means sharing, employing, applying, utilizing, examining, or analyzing PHI within IDG

⁴Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG

Related Forms:

Authorization for Release of Information Form

Related Policies:

Subpoenas and Court Orders-CC-P-020

References:

45 CFR §164.514(h)-Verification Requirements

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-010
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Patient Right to Request and Accounting of Disclosures
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce², independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

Upon request, IDG shall provide individuals with a list of disclosures (an accounting) that were made to other organizations or entities by IDG by law or regulation.

Policy & Procedure:

1. A patient has the right to receive a listing (accounting) of disclosures of his or her health information. All requests for an accounting will be handled by the Legal Department of Privacy Officer. Patient must request an accounting in writing by completing the Request for Accounting form and submitting it to the Legal department or the Privacy Officer.
2. IDG does not need to account for the following disclosures:
 - a. Disclosures made prior to April 14, 2003
 - b. Disclosures made for treatment, payment, or healthcare operations
 - c. Disclosures made pursuant to the patient's authorization
 - d. Disclosures made to the patient or representative
 - e. Disclosures for persons directly involved in the patient's care
 - f. Disclosures that are incidental to an otherwise permitted disclosure
 - g. Disclosures for national security or intelligence purposes
 - h. Disclosures to correctional institutions or law enforcement officials regarding persons in custody
 - i. Disclosures pursuant to a limited data set²

3. Examples of disclosures that must be tracked and accounted for include disclosures to/or for:
 - a. Governmental authorities required by law for abuse, neglect and domestic violence
 - b. Health oversight activities required by law to audit and investigate³
 - c. Governmental authorities required by law for child abuse or neglect
 - d. Law enforcement officials concerning crime victims or criminal conduct
 - e. Coroner or medical examiner required by law for a decedent
 - f. Public authority required by law for disease reporting
 - g. The Food and Drug Administration
 - h. Public health authorities required by law to collect information regarding injury or disability
 - i. Organ procurement
 - j. Research purposes (except if the patient signed an authorization)
 - k. Pursuant to a subpoena, discovery request, or a court order
 - l. Aversion of threats to public health or safety
 - m. Administration of the Department of Veteran Affairs
 - n. Public health authorities required by law to collect vital statistics.

4. An accounting must include the following information:
 - a. The date of the disclosure
 - b. The name of the entity or person who received the PHI, and, if known, their address
 - c. A brief description of the health information disclosed
 - d. A brief statement of the purpose of the disclosure

5. Timing. IDG must provide an accounting no later than 60 days after receiving the patient's request.
 - a. If IDG cannot meet the 60-day deadline, IDG may extend the deadline by 30 days if ADG informs the individual of the extension in writing within the original 60-day deadline
 - b. IDG's extension notice must state the reason for the delay and the date in which you will provide the requested accounting. IDG may only extend the deadline once.

6. Fees. The first accounting in any 12-month period will be provided free of charge. IDG may invoice for future reports requested within the 12-month period.

7. Documentation. For six (6) years, IDG must document and retain the information included in the accounting to an individual, a copy of the accounting that was provided to the individual, and the title of the person or office responsible for receiving and processing the accounting.

8. Denying a Request for an Accounting. IDG can deny a request for an accounting when made by the personal representative of a patient if:
- a. The patient has been or may be subject to domestic violence, abuse, or neglect by the person requesting the information and the accounting could endanger the patient
 - b. The Legal Department or the Privacy Officer decides that it is not in the best interest of the patient to treat the person as the patient's representative.

¹Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

²Limited Data Set is PHI that excludes the following direct identifiers of the individual or of relatives, employers or household member of the individual: names, postal address information, other than city or town, state and zip code; telephone number; fax numbers; email addresses; Social Security Number; medical record number; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; URLs; IP addresses; biometric identifiers, including finger and voice prints; and full-face photographic images and any comparable images.

³If you are disclosing patient's health information to law enforcement officials or a health oversight agency and the agency or official provides you with a statement indicating that disclosure in the accounting would impede their investigation, you must exclude this disclosure from your accounting.

Related Forms:

Request for Accounting of Disclosures of PHI
Notice of Privacy Practices

Related Policies:

Privacy Officer-CC-P-003
Permitted Uses and Disclosures of PHI-CC-P-004
Notice of Privacy Practices-CC-P-007

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-011
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Business Associate ("BA") ¹ Policy
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce², independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

To secure business associate contacts with all persons or entities that provide services for or on behalf of IDG who will have access to or create protected health information ("PHI")³. Business Associate Agreement ("BAA")⁴ are required by HIPAA to ensure that the business associate takes appropriate steps to safeguard PHI.

Policy & Procedure:

1. Identifying a Business Associate. Determine if the person or entity you are contracting with, or entering into a purchase agreement with, or entering into a purchase agreement with, is a BA.
 - a. BAs can be defined in a two-part set:
 1. A contractor who receives PHI from IDG
 2. For the purpose of assisting with or performing a function for or on behalf of IDG.
 - b. BA relationship exists when the BA performs a function that the covered entity⁴ could not perform for itself.

2. Complete the BAA. Complete the appropriate fields of the BAA for each BA and obtain a signed agreement. If you are unsure whether a BAA is needed, contact the Privacy Officer/Compliance Officer or Legal Department for guidance.
 - a. When possible, always use the IDG BAA opposed to the BA's form
 - b. If the BA requests changes to the IDG BAA or insist on using their own form, contact the Privacy Officer/Compliance Officer, or Legal Department for review.

3. A BAA is NOT required for disclosures to:
 - a. Treatment providers involved in the patient's care
 - b. Health plans for payment
 - c. Members of the workforce
 - d. Janitorial, housekeeping companies
 - e. Delivery companies such as Federal Express, USPS
 - f. Any vendor that does not have access to IDG PHI

4. The IDG BAA template contains statement that are required by law. Changes to the IDG BAA template must be approved by the Privacy Officer/Compliance Officer or the Legal Department.

5. If IDG uncovers or knows of a pattern of activity or practice of the BA that constitutes a material breach or violation of the BA's obligations under the BAA, IDG must take reasonable steps to remedy the BA's breach or end the BA's violation.

6. IF the BA does not cease the breach/violation, the Privacy Officer and Legal Department, must take one of two actions:
 - a. Terminate the agreement or contract, if feasible
 - b. If termination is not feasible, the violation/breach should be reported to the Secretary of the Department of Health and Human Services.

7. IDG will comply with the reporting guidelines as outlined in the Department of Health and Human Services breach reporting guidelines for BAs.

8. In the course of business there may instances where IDG would be held as the BA in a relationship. IDG will perform all duties as the BA and sign any necessary agreements as the BA.

¹Business associate means a person or entity that may use or disclose PHI to perform a function or activity on behalf of IDG. A business associate is not a member of the workforce.

²Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

³Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

⁴Business Associate Agreement ("BAA") means an agreement made between IDG and business associates who have access to PHI.

Related Forms:

IDG Business Associate Agreement Template

Related Policies:

Privacy Officer-CC-P-003

Breach Notification Policy-CC-P-024

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-012
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Patient's Right to Request an Amendment of Protected Health Information ("PHI") ¹
Effective:	11/1/21
Approval:	10/23/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce², independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

Each patient has the right to request that IDG amend PHI or a record about the patient contained in the patient's designation record set for as long as the PHI is maintained by IDG.

Policy & Procedure:

1. Patient's Amendment Request
 - a. Each patient has the right to request that IDG amend PHI on a record about the patient contained in the patient's designated record set for as long as the PHI is maintained by IDG.
 - b. A patient must submit any request for amendment of his/her PHI
 1. IDG offers to provide the patient with the form, Request for Amendment;
 2. IDG also may accept, in its reasonable discretion, other forms of amendment requests. IDG will not unreasonably deny a patient's request to amend the patient's PHI if the request identifies the PHI in the record for which the patient would like an amendment and the reason(s) for the patient's amendment request.
 - c. If a member of the workforce receives a patient amendment request, he/she immediately directs the request to the IDG Privacy Officer.
 - d. The IDG Privacy Officer (or delegate) review the request and discusses with the appropriate individual(s) or department(s) within IDG that created the entry in the patient's record to which an amendment has been requested.

- e. IDG acts on the patient's amendment request within 60 days of receiving the request, unless IDG sends an extension notice to the patient. If IDG is unable to act on a patient's amendment request within 60 days of its receipt, IDG may extend its time for responding to a patient's amendment request by 30 days, provided that the IDG Privacy Officer (or delegate) sends a letter to the patient explaining the reason(s) for the delay and the expected date the decision will be made (which must be within the additional 30-day period). Not additional extensions are permitted.

2. Granting a Patient's Amendment Request

- a. IDG will take the following steps when granting a patient's amendment request in whole or in part;
 - 1. The IDG Privacy Officer (or delegate) and the individual(s) responsible for amending the PHI identifies the PHI to be changed as well as the records that are affected by the amendment.
 - 2. The individual(s) responsible for amending the PHI append the amendment to the original PHI or record or provide a link to the location of the amendment. Under no circumstances may information be deleted from the patient's record. However, if the wrong patient's information was placed into another patient's record, such information is moved to the appropriate patient's record.
 - 3. The IDG Privacy Officer (or delegate) informs the patient in writing that the amendment has been granted. If the patient has identified persons or entities that should receive the amended information, the approval letter will indicate whether IDG has complied with the patient's request.
 - 4. The IDG Privacy Officer (or delegate) makes reasonable efforts to inform and provide the amendment (within a reasonable time) to;
 - a. The persons identified by the patient as needed the amended information.
 - b. Persons, including Business Associates³ of IDG that IDG knows has the PHI that is subject of the amendment and that may have relied, or could foreseeably rely on such information to the detriment of the patient.

3. Reasons for Denying a Patient's Amendment Request

- a. IDG may deny a patient's amendment request if the PHI on record meets one of the following conditions
 - 1. The PHI on record was not created by IDG;
 - 2. The PHI is not part of the designated record set
 - 3. The PHI is accurate and complete.

4. Denying a Patient's Amendment Request
 - a. IDG takes the following steps when denying a patient's amendment request in whole or in part;
 1. The IDG Privacy Officer (or delegate) informs the patient in writing, that the request was denied. The letter include the following information.
 - a. The reason for the denial
 - b. The patient's right to submit a written statement of disagreement with IDG's decision and how the patient may file such a written statement
 - c. A statement that, if the patient does not submit a written statement disagreement, the patient may request that IDG provide the patient's amendment request and IDG's denial with any future disclosures of the PHI that are subject of the patient's amendment request
 - d. A description of how the patient may complain to IDG, including the name or title, and telephone number of the individual sending the denial letter; or to the Secretary of the Department of Health and Human Services. The detailed information necessary to inform the patient how to submit a complaint to the Secretary of the Department of Health and Human Services includes the following;
 1. The patient's complaint must be filed in writing, either or paper or electronically;
 2. The patient's complaint must name IDG as the subject of the complaint and describe the acts or omissions believed to be in violation of HIPAA;
 3. A complaint must be filed within 180 days of when the patient knew or should have known the act of omission complained of occurred, unless this time is waived by the Secretary for good cause.
 2. IDG permits the patient to submit a written statement disagreeing with the denial of all of or part of the requested amendment and the basis of such disagreement;
 - a. IDG may reasonably limit the length of a statement of disagreement.
 3. IDG may prepare a written rebuttal to the patient's statement of disagreement.

¹Protected Health Information (“PHI”) contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

²Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

³Business associate means a person or entity that may use or disclose PHI to perform a function or activity on behalf of IDG. A business associate is not a member of the workforce.

Related Forms:

Request for Amendment of PHI

Related Policies:

Privacy Officer-CC-P-003

Resources:

45 CFR §164.526-Amendment of Protected Health Information

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-013
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Privacy Training for Workforce Members ¹
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG will provide initial training to workforce members on IDG's policies and procedures regarding protected health information ("PHI")² and patient privacy during their orientation or as soon as possible after their start date.

IDG will train workforce members whose functions are affected by a substantive change in privacy and procedures as soon as possible after the change is effective.

IDG will train all workforce members annually regarding IDG's policies and procedures regarding PHI and patient privacy.

IDG will document the type, amount and dates of training received by workforce members and retain this information for at least six years from the date of training.

Policy & Procedure:

1. Initial Training of Workforce Members
 - a. IDG will provide initial training to workforce members on IDG's policies and procedures regarding PHI and patient privacy during their orientation or as soon as possible after their start date.
 1. Workforce members receive initial privacy training during the orientation sessions facilitated by the Human Resources Department.
 2. The training can be in person or electronically.

2. Subsequent Privacy Training
 - a. IDG will train workforce members whose functions are affected by a substantive change in privacy policies and procedures as soon as possible after the change is effective.
 - b. EDG provides annual compliance training to all members of the workforce, which includes additional privacy training.

 3. Documentation of Privacy Training
 - a. IDG will document the type, amount and dates of training received by workforce members and retain this information for at least six years from the date of training.
-

¹Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

²Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

Related Policies:

Privacy Officer-CC-P-003

Resources:

45 CFR §164.530(b)-Privacy training standards

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-014
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Patient's Right to Request Privacy Restrictions
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce¹, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

Each patient has the right to request certain restrictions on how their protected health information ("PHI")² may be used³ or disclosed⁴. All requests for such restrictions must be made in writing to the IDG Privacy Officer.

Policy & Procedure:

1. Patient's Right to Request Privacy Restrictions
 - a. IDG permits patients to request restriction on how their PHI may be used or disclosed for the following purposes:
 1. For treatment, payment or healthcare operations
 2. To individuals involved in the patient's care (such as a family member, friend or someone else identified by the patient)
 3. To notify a family member, friend, or someone else involved in the patient's care of the patient's location, general condition or death.
 - b. IDG is not required to agree to any of the above restriction requests.
 - c. All patient restriction requests must be made in writing using the Request for Restrictions form. A reasonable handwritten explanation will also be accepted.
 - d. No workforce member or physician is permitted to grant or deny a patient restriction request without prior consultation with IDG Privacy Officer (or delegate).

2. Honoring a Patient's Request for Privacy Restrictions
 - a. If IDG agrees to the request, IDG documents the restriction in the patient's record.
 - b. IDG complies with the agreed-upon restriction unless applicable law otherwise requires disclosure.

3. Terminating the agreement to restrict the use and disclosure of PHI.
 - a. The IDG Privacy Officer (or delegate) or patient may terminate the agreement to restrict the use or disclosure of PHI under the following circumstances:
 1. The patient requests in writing that the restriction be terminated.
 2. The patient verbally agrees to terminate the restrictions, in which case the IDG Privacy Officer (or delegate) documents the patient's agreement to terminate the restriction in the patient's record.
 3. The IDG Privacy Officer (or delegate) informs the patient the agreement to restrict PHI has been terminated; however;
 - a. PHI gathered during the term of the restriction will continue to be restricted.
 - b. PHI gathered after the termination of the agreement will not be restricted.

¹Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

²Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

³Use means sharing, employing, applying, utilizing, examining or analyzing PHI within IDG

⁴Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG

Related Forms:

Request for Restriction of Use and Disclosure of PHI

Related Policies:

Privacy Officer-CC-P-003

Resources:

45 CFR §164.522(a)-Right of an individual to request restriction of uses and disclosures

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-015
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	De-Identifying Protected Health Information ("PHI") ¹
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce², independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

De-identified health information³ is not PHI and is not subject to HIPAA rules and regulations.

IDG workforce members may create de-identified health information from PHI per this policy.

IDG workforce members are permitted to disclose PHI to a business associate⁴ to create de-identified health information after the business associated has signed a business associate agreement⁵ in for acceptable to IDG.

Once PHI is de-identified, a patient's authorization is not necessary to use⁶ or disclose⁷ the de-identified health information.

Policy & Procedure:

1. Creation of De-Identified Health Information
 - a. IDG workforce members may create di-identified health information from PHI using on of the methods listed below:
 1. A person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.
 - a. Applies such principles and methods to determine that the risk is very small that the information would be used, alone or in combination with other reasonably available information, by a recipient to identify the individual who the subject of the information.

- b. Documents the methods and results of the analysis that justify such determination.
2. All of the following identifiers of the patient, relative, employers or household members of the patient, are removed and IDG does not have knowledge that the information could be used alone or together with other information to identify an individual.
- a. Names
 - b. All geographic subdivision smaller than a state, including street address, city , county, precinct, township, zip code and their equivalent geocodes, except the first three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census, the geographic unit formed by combing all zip code with the same three initial digits contains more than 20,000 people and the first three digits of a zip code for all geographic units containing 20,000 or few people is changed to 000.
 - c. All element of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages of 89 years old and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a singed category of age 90 years or older.
 - d. Telephone Numbers
 - e. Fax Numbers
 - f. Email addresses
 - g. Social Security Numbers
 - h. Medical Record Numbers
 - i. Health plan beneficiary numbers
 - j. Account Number
 - k. Certificate/License Numbers
 - l. vehicle identifiers and serial numbers; including license plate numbers
 - m. Device identifiers and serial numbers
 - n. Web Universal Resource Locators (URLs)
 - o. Internet Protocol (IP) address numbers
 - p. Biometric Identifiers, including finger and voice prints
 - q. Full face photographic images and any comparable image
 - r. Any other unique identifying number, characteristic or code; except for a code to allow IDG to re-identify the information.
- b. IDG workforce members are permitted to disclose PHI to a business associate to created de-identified health information only aft the business has signed a business associate agreement in a form acceptable to IDG.

2. Use and Disclosure of De-Identified Health Information
 - a. De-identified health information is not PHI and is not subject to HIPAA protections.
 - b. Once PHI is de-identified, a patient's authorization is no longer necessary to use or disclose the de-identified health information.
 - c. Prior to disclosing de-identified health information, IDG may code the information to allow IDG to re-identify the information.
 1. The code or other method of identification is not created from or related to information about any patient.
 2. The code or other method of identification cannot be translated to identify any patient
 3. The code or other method of identification is not disclosed to the recipient of the de-identified health information or to any other person/entity.
-

¹Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

²Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

³De-identified is health information that does not identify a patient and which IDG does not reasonably believe can be used to identify a patient.

⁴Business Associate means a person or entity that uses or discloses PHI to perform a function or activity on behalf of IDG. A business associate is not a member of the workforce. All business associates must sign a business associate agreement satisfactory to IDG before providing any services to or on behalf of IDG.

⁵Business Associate Agreement ("BAA") means an agreement made between IDG and business associates who have access to PHI.

⁶Use means sharing, employing, applying, utilizing, examining or analyzing PHI within IDG

⁷Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG

Related Policies:

Business Associate-CC-P-011

Resources:

45 CFR §164.514(a)-(c)-Other requirement relating to uses and disclosure of PHI

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-016
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Limited Data Set: Permitted Purposes for Use/Disclosure
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC (“IDG”), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce¹, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG may use² or disclose³ protected health information (“PHI”)⁴ to create a limited data set⁵ for research⁶, public health or healthcare operation purposes only. The limited data set may be disclosed to a third party only after the recipient has signed a data use agreement in a form acceptable to IDG.

IDG may disclose PHI to a business associate⁷ to create a limited data set, provided that the business associate has signed a data use agreement in a form acceptable to IDG.

Policy & Procedure:

1. Creation of a Limited Data Set (“LDS”)
 - a. IDG may use or disclose PHI to create a LDS for research, public health or healthcare operations purposes only.
 - b. An LDS may be disclosed to a third party only after the recipient has signed a data use agreement (“DUA”) in a form acceptable to IDG. IDG legal counsel must approve, in writing, any DUA prior to its execution.
 1. IDG may disclose PHI to a business associate to create an LDS, when there is a written contract and business associate agreement⁸.
 2. An individual entering into a DUA that is not approved in advance by IDG legal counsel is a violation of this policy and the DUA may be deemed to be unenforceable.
 - c. A DUA must include all of the following requirements:
 1. Establish the permitted uses and disclosures of the LDS set by the recipient, consistent with the purposes of the disclosure, and which may not include any use or disclosure that would violate HIPAA if done by IDG.

2. Limit who can use or receive the data
3. Require the LDS recipient to agree to all of the following provisions:
 - a. Not so use or disclose the information other than as permitted by the DUA or as otherwise required by law.
 - b. Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the DUA.
 - c. Report in writing to IDG any use ,disclosure or breach of the information not provided for by HIPAA or the DUA of which the recipient know or should have known.
 - d. Ensure that any agents or subcontractors, to whom the recipient provide the LDS agrees to the same restrictions and conditions that apply to the recipient with respect to the LDS.
 - e. Not to re-identify the information or contact the patients who are the subjects of the LDS.
- d. If IDG knows of, or is aware of a material breach or violation of a DUA by the creator or recipient of an LDS, IDG must take reasonable steps to cure the breach, report the breach, if necessary or end the agreement. If these efforts are unsuccessful, IDG must take both the following steps:
 1. Discontinue disclosure of the LDS to the recipient
 2. Consult with IDG legal counsel or the Compliance Officer to report the problem to the Secretary of the Department of Health and Human Services.

¹Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

²Use means sharing, employing, applying, utilizing, examining or analyzing PHI within IDG

³Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG.

⁴Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

⁵A limited data set (LDS) is PHI that has all of the following 16 direct identifiers of the patient or relatives, household member or employers removed:

- a. Names
- b. Post address information, other than town or city, state and ZIP code
- c. Telephone Numbers
- d. Fax Numbers
- e. Email Addresses
- f. Social Security Numbers
- g. Medical Records/Prescription Numbers
- h. Health Plan Beneficiary Numbers
- i. Account Numbers
- j. Certificate/License Numbers
- k. Vehicle Identifiers and Serial Numbers, including License Plate Numbers
- l. Device Identifiers and Serial Numbers
- m. Web Universal Resource Locators (URLs)
- n. Internet Protocol (IP) Address Numbers
- o. Biometric Identifiers, including Finger and Voice Points
- p. Full Face Photographic Images and any Comparable Images

⁶Research means systematic investigation, including research development, testing and evaluation, designed to develop or contribute to general knowledge.

⁷Business Associate means a person or entity that uses or discloses PHI to perform a function or activity on behalf of IDG. A business associate is not a member of the workforce. All business associates must sign a business associate agreement satisfactory to IDG before providing any services to or on behalf of IDG.

⁸Business Associate Agreement (“BAA”) means an agreement made between IDG and business associates who have access to PHI.

Related Policies:

Business Associate-CC-P-011

Breach Notification Policy-CC-P-024

Resources:

45 CFR §164.514(e)(1)-Standard: Limited Data Set

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-017
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Uses ¹ and Disclosures ² of Protected Health Information (“PHI”) ³ for Marketing ⁴
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC (“IDG”), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce⁵, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG shall limit the use and disclosure of PHI for marketing activities to that which is permissible under the HIPAA Privacy Rule.

Policy & Procedure:

1. IDG obtains written authorization from patients before using or disclosing their PHI for marketing purposes.
 - a. A limited exception to this requirement applies when marketing:
 1. Occurs during an in-person meeting between IDG and the patient.
 2. Is limited to IDG providing a promotional gift of nominal value (such as a coffee cup or key ring) to the patient.
 - b. Requests to obtain an authorization form for marketing purposes should be directed to the IDG Privacy Officer or the Marketing Department.
2. Communications may be in the form of a newsletter or similar general communications that IDG distributes to a broad cross-section of patients or similar broad groups of individuals. Communications may include information about IDG’s services and testimonies.
 - a. Any marketing communication to individuals may not include or promote a third-party product.
 - b. IDG is authorized to disclose PHI to a business associate⁶ to assist with marketing, but the business associate agreement⁷ must assure that the business associate will not use or disclosure the PHI for any other purpose.

3. The following types of IDG communications are not considered marketing:
 - a. Communications that describes a health-related product or service IDG offers.
 - b. Communications for treatment purposes.
 - c. Communications for case management or care coordination purposes.
4. IDG will describe in the Notice of Privacy Practices⁸ any marketing activities that use patient information not requiring a specific authorization.
5. IDG makes reasonable efforts to ensure that those patients who do not want to receive marketing materials are removed from any marketing mailing list.

¹Use means sharing, employing, applying, utilizing, examining, or analyzing PHI within IDG

²Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG.

³Protected Health Information (“PHI”) contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

⁴Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

⁵Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

⁶Business Associate means a person or entity that uses or discloses PHI to perform a function or activity on behalf of IDG. A business associate is not a member of the workforce. All business associates must sign a business associate agreement satisfactory to IDG before providing any services to or on behalf of IDG.

⁷Business Associate Agreement (“BAA”) means an agreement made between IDG and business associates who have access to PHI.

⁸Notice of Privacy Practice (NPP) is a general description of the patient’s rights with respect to PHI, how IDG may use and disclose PHI and IDG’s legal duties with respect to PHI.

Related Forms:

Notice of Privacy Practice

Related Policies:

Business Associate-CC-P-011

Notice of Privacy Practice-CC-P-007

Resources:

45 CFR §164.508-Uses and disclosures for which an authorization is required

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-018
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Uses ¹ and Disclosures ² of Protected Health Information (“PHI”) ³ for which an Authorization ⁴ from the Patient is not Required
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC (“IDG”), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce⁵, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG may use or disclose PHI without an authorization or the opportunity for the patient to agree or object, in the situations covered by this policy, subject to the applicable requirements of this policy. When IDG is required by this policy to inform the patient of, or when the patient may agree to a use or disclosure permitted by this section, IDG’s information and the patient’s agreement may be given orally.

Policy & Procedure:

1. Public Health Activities
 - a. A Public Health Authority⁶
 1. To prevent or control a disease, injury, or disability (including reporting of a disease, injury, vital events such as birth or death)
 2. To conduct public health surveillance, investigations, and interventions.
 3. At the discretion of a Public Health Authority, IDG may disclose PHI to an official of a foreign government agency acting in collaboration with a public health authority.
 - b. A Public Health Authority (or other government authority) authorized by the law to receive report of child abuse or neglect and elderly abuse or neglect.

- c. A person subject to Food and Drug Administration (“FDA”) jurisdiction with respect to an FDA-regulated product or activity for which that person has responsibility, for the purposes of activities related to the quality, safety or effectiveness of FDA-regulated product or activity. These purposes include:
 - 1. Collecting or reporting adverse events) or similar reports relating to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product).
 - 2. Track FDA-regulated products.
 - 3. Enable product recalls, repairs, replacement, or look back (including efforts to locate and notify patient who have received products that are withdrawn, recalled or are subject of a look back).

- 2. Uses and Disclosures for Health Oversight Activities
 - a. IDG may disclose PHI to a Health Oversight Agency for oversight activities authorized by law (including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil administrative or criminal proceedings or actions) or other activities necessary for appropriate oversight of:
 - 1. The healthcare system.
 - 2. Government benefit programs relevant to beneficiary eligibility.
 - 3. Government regulatory programs for determining compliance with program standards.
 - 4. Entities subject to civil rights laws for which PHI is necessary for determining compliance.
 - b. IDG may NOT provide PHI if the patient is the subject of the investigation, unless the investigation arises out of and is directly related to the patient’s receipt of healthcare; a claim for public benefits by the patient related to health; or the qualification for or receipt of public benefits or services when a patient’s health is integral to the claim for public benefit or services.

- 3. Uses and Disclosures Required by Law
 - a. IDG may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
 - 1. Disclosures regarding victims of abuse, neglect, or domestic violence: IDG may disclose PH about a patient whom IDG reasonably believes to be a victim of abuse, neglect, or domestic violence to a governmental authority, including a social service or protective service agency authorized by law to receive report of such abuse, neglect or domestic violence, if one of the following conditions apply:

- a. To the extent the disclosure is required by law and the disclosure complies with an is limited to the minimum necessary amount of PHI necessary to comply with the law.
 - b. If the patient agrees to the disclosure; and such agreement may be an oral agreement (should be documented in the medical record).
 - c. To the extent the disclosure is expressly authorized by statute or regulation and:
 - 1. The workforce member makes the disclosure, in the exercise of professional judgement believes the disclosure necessary to prevent serious harm to the patient or other potential victims or;
 - 2. If the patient is unable to agree due to incapacity, a law enforcement or other public official authorized to receive the report represent that the PHI for which the disclosure is sought is not intended to be used against the patient and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the patient is able to agree to the disclosure.
 - 3. The workforce member making the disclosure will inform the patient (or personal representative) that report has been or will be made, unless:
 - a. The workforce member (in the exercise of his/her professional judgement or in the professional judgement of the attending physician) believes that informing the patient would create the risk of serious harm to the patient: or
 - b. The workforce member would be notifying the patient's personal representative who the workforce member reasonable believe is responsible for the abuse, neglect or injury and that information the personal representative, in the workforce member's professional judgment would not be in the best interest of the patient.
- b. Disclosures for judicial and administrative proceedings.
- 1. In response to an order of a court of administrative tribunal (including a subpoena, discovery request, or other lawful process that is accompanied by an order of court or administrative tribunal).
 - 2. In response to subpoena with an appropriate authorization from the patient or from the patient's personal representative.

- c. Disclosures for Law Enforcement purposes.
1. IDG may disclose PHI as required by law (including laws that require the reporting of certain types of injuries except for disclosures about victims of abuse, neglect or domestic or child abuse), which are dealt with in Section 1 or Section 3(a)(1) of this policy or in compliance with and as limited by the relevant requirements of:
 - a. A court order, court-ordered warrant, subpoena, summons issued by a judicial officer, grand jury subpoena, or:
 - b. A governmental request, including an administrative subpoena or summons, if the following conditions are satisfied:
 1. The information sought is relevant and material to a legitimate law enforcement inquiry.
 2. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.
 3. De-identified information could not reasonably be used to fulfill the request.
 2. IDG may disclose PHI to a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness or missing person if the disclosure of PHI is limited to:
 - a. Name and Address
 - b. Date and Place of Birth
 - c. Social Security Number
 - d. Blood Type and Rh Factor
 - e. Type of Injury
 - f. Date and Time of Injury
 - g. Date and Time of Death, if applicable
 - h. A description of distinguishing physical characteristics
 3. IDG will not disclose any PHI related to the patient's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue for the purpose of identification.
 4. A workforce member that is the victim of a criminal act may disclose PHI to a law enforcement official if:
 - a. The PHI disclosed is about the suspected perpetrator of the criminal act, and:
 - b. The PHI disclosed is limited to the items set forth in 3C (2)

5. Except for disclosures required by law, IDG may disclose PHI about a patient in response to a law enforcement official's request if:
 - a. The patient is (or suspected of being) a victim of a crime and the patient agrees to the disclosure (the patient agreement should be documented in the medical records) or:
 - b. IDG cannot obtain the patient's agreement because of incapacity or other emergency circumstances but the disclosure is in the best interest of the patient as determined by IDG in the exercise of professional judgement and the law enforcement official represents that:
 1. The PHI is necessary to determine whether a violation of law (by a person other than the victim) occurred; and
 2. Immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the patient is able to agree to the disclosure.
 6. IDG may disclose PHI about a patient who has died to a law enforcement official if IDG suspect that the death may have resulted from criminal activity.
 7. IDG may disclose PHI to a law enforcement official that IDG believes in good faith that such PHI constitutes evidence of criminal conduct that occurred on the premises of a facility.
4. Use and Disclosures about Decedents
 - a. IDG may disclose PHI to a coroner or medical examiner for the purposes of identifying a deceased person, determining the cause of death or other duties as authorized by law.
 - b. As is consistent state law, IDG may disclose PHI with respect to a deceased patient to a funeral director as necessary. If necessary, for funeral directors to carry out their duties, IDG may disclose the PHI prior to, and in reasonable anticipation of the patient's death.
 5. Uses and Disclosure for Cadaveric Organ, Eye or Tissue Donation Purpose
 - a. IDG may disclose PHI for or to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.
 6. Uses and Disclosures to Avert a Serious Threat to Health and Safety
 - a. IDG may, consistent with applicable law and standards of ethical conduct, use or disclose PHI, if IDG, in good faith, believe the use of disclosure:

1. Is necessary to prevent or lessen a serious an imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
 2. Is necessary for law enforcement authorities to identify or apprehend a patient:
 - a. Because of a statement by the patient admitting participation in a violent crime that IDG reasonably believes ma have cause serious physical harm to the victim (but any such disclosure of PHI is limited to the information set forth in section 3C (2)
 - b. Where it appears from all the circumstances that the patient has escaped from a correctional institution or from lawful custody.
7. Uses and Disclosure of Specialized Government Functions
- a. IDG may use and disclose PHI of patients that are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of a military mission. Prior to disclosure, the IDG legal counsel or Privacy Officer must confirm, in writing, that the appropriate publication requirements have been satisfied.
 - b. IDG may use and disclose the PHI of patient who are foreign military personnel for or to their appropriate foreign military authority.
 - c. IDG may use and disclose PHI to authorized federal officials who are conducting lawful intelligence, counterintelligence or other nation security activities authorized by the National Security Act and implementing authority. Prior to the disclosure, the IDG legal counsel mu approve the disclosure in writing.
 - d. IDG may disclose PHI to authorized federal officials to provide protective services to the President of the United States, to foreign heads of state or for the conduct of certain investigations authorized by the United States. Prior to disclosure, the IDG legal counsel must approve the disclosure in writing.
 - e. IDG may disclose to a correctional institution (or a law enforcement official having lawful custody of an inmate or other patient) PHI about such inmate or patient if the correctional institution or such law enforcement officials represents that such PHI is necessary for:
 1. The provision of healthcare to such patients.
 2. The health and safety of such patient or other inmates.
 3. The health and safety of the officers or employees of or others at the correctional institution
 4. The health and safety of such patients and officers or other persons responsible for the transporting of inmates on their transfer from one institution, facility or setting to another.
 5. Law enforcement on the premises of the correctional institution.
 6. The administration and maintenance of the safety, security, and good order of the correctional institution.

7. For the purposes of this policy, a patient is no longer an inmate when released on parole, probation, or supervised release, or otherwise is no longer in lawful custody.

8. Disclosures of Workers' Compensation

- a. IDG may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law that provide benefits for work-related injuries or illnesses without regard to fault.

¹Use means sharing, employing, applying, utilizing, examining, or analyzing PHI within IDG

²Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG.

³Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

⁴An authorization means a detailed document that gives IDG permission to use PHI for specified purposes, which are generally other than treatment, payment, and healthcare operations, or to disclose PHI to a third-party specified by the individual.

⁵Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

⁶Public Health Authority means an agency of the United States, or a person, entity, employee, agent, or subcontractor acting under a grant of authority from or contract with such agency, if the agency is responsible for public health matters as part of the agency's official mandate

Related Forms:

Authorization for Release of PHI

Notice of Privacy Practice

Related Policies:

Notice of Privacy Practice-CC-P-007

PHI restrictions Requested by Patient-CC-P-014

De-Identifying PHI-CC-P-015

Complaint and Reporting Policy-CC-P-023

Resources:

45 CFR §164.530-Administrative Requirements

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-019
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Privacy and Security of Non-Electronic ¹ Protected Health Information ("PHI") ²
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce³, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG takes all reasonable steps to secure the privacy and security of non-electronic PHI.

Policy & Procedure:

1. IDG established appropriate procedures governing the removal of non-electronic PHI from departments within IDG by workforce members. These procedures include all the following requirements:
 - a. Workforce members must have a legitimate, work-related purpose for removing PHI from IDG.
 - b. Before a workforce member is permitted to remove PHI from IDG, his/her supervisor must provide advanced approval, as well as guidance on the individual's responsibility to protect the PHI while it is her/his possession.
 - c. Workforce members are responsible for the privacy and security of the PHI while it is outside of IDG and take the following steps to secure the PHI:
 1. An individual transporting PHI by vehicle keeps the vehicle locked and placed the PHI in the trunk or other locations so that the PHI is hidden from plain sight.
 2. An individual mailing PHI must accurately and legibly address and securely seals the envelope.
 3. If an individual leaves PHI unattended in an area that is highly accessible to visitors in anticipation that another individual will retrieve it, the individual places the PHI in a sealed envelope containing the recipient's name.
 - d. An individual only removes the minimum necessary PHI to perform the job or function that necessitates the PHI being removed from IDG.

- e. After removing PHI from IDG, an individual returns the PHI to IDG as soon as possible after completing the work-related task.
 - f. Any PHI removed from IDG is returned promptly to IDG for retention or appropriate destructions.
 - g. Upon termination of an individual's relationship with IDG, the individual immediately returns all PHI removed from IDG.
2. Any lost or stolen PHI should be reported immediately to the Privacy Officer.
-

¹Non-electronic PHI means PHI that is contained in a tangible format, such as paper records and films. Non-electronic PHI includes electronic PHI that is converted into a tangible format.

²Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

³Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

Related Policies:

Breach Notification Policy-CC-P-024

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-020
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Subpoenas and Court Orders
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC (“IDG”), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce¹, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG is required by law to comply with any properly executed Court Order, Subpoena, or other valid requests for documents.

IDG must protect their patient’s right to confidentiality and privacy.

Policy & Procedure:

1. IDG is required by law to comply with any properly executed Court Order, Subpoena, or other valid request for documents and/or testimony regarding their patients as it related to services provided.
2. All Subpoenas should be forwarded to Legal/Compliance or Privacy Officer.
3. Subpoenas
 - a. Subpoenas for Medical Records or Bills:
 1. If confidential medical information or billing is requested; the Subpoena must be determined to be valid. The subpoena must be signed by a Judge, Magistrate, Clerk of Courts or an attorney in some states. This signature can usually be found at the bottom right-hand corner of the document. If signed by a Judge or Magistrate, no HIPAA release is required. The records can be released. If signed by an attorney, stat statutory requirements mandate a waiting period before records are released. If records and/or bills are requested, they should be forwarded to the person and address listed on the subpoena.

2. A specific release is required for psychiatric/psychological records. This release will specifically state that psychiatric/psychological records are requested.
- b. Request for Medical Records and/or Bills:
 1. A patient and/or a patient's attorney can request medical bills/records in the form of a letter to the provider accompanied with a valid HIPAA Authorization.
 2. The HIPAA Authorization must be valid and made to the appropriate entity.
 3. Once the HIPAA Authorization is determined valid, records can be disclosed to the patient and/or the patient's attorney.
 - c. Request for Subpoena for Treating Provider Deposition or Trial Testimony, Grand Jury Subpoenas.
 1. An attorney may request or issue a subpoena for deposition and/or trial testimony of a treating provider. All of these must be directed to IDG Legal.
 2. IDG Legal will coordinate the testimony and make sure that all protections are in place for the provider.
 3. A valid HIPAA Authorization is required if an attorney wants to talk about or address any patient care/treatment information prior to or after the actual testimony.
 - d. Subpoenas in a Medical Malpractice Case where IDG is not a Defendant
 1. If an IDG provider is subpoenaed for deposition or trial testimony in a medical malpractice case where he or she is not named a defendant, but treated the patient, IDG Legal should be contacted.
 - e. All other Subpoenas
 1. Any and all other subpoenas, including but not limited to subpoenas for employment records will be sent to IDG Legal.

¹Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

Related Policies:

Authorization for use and Disclosures-CC-P-002

Minimum Necessary Requirements-CC-P-006

Uses and Disclosures of PHI for which an Authorization is not Needed-CC-P-018

Resources:

45 CFR §164.514(e)(1)-Standard: Limited Data Set

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-021
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Uses ¹ and Disclosures ² of Protected Health Information ("PHI") ³ for Treatment ⁴ , Payment ⁵ or Healthcare Operations ⁶
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce⁷, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG workforce members may use or disclose PHI for purposes of treatment, payment, and healthcare operations, but such uses, and disclosures are subject to the minimum necessary uses and disclosures.

Policy & Procedure:

1. Examples of Treatment:
 - a. Coordination or management of healthcare by a healthcare provider with a third party or consultation.
 - b. Referrals between one healthcare provider to another.

2. Examples of Payments:
 - a. Verification of eligibility or coverage
 - b. Risk Adjustments
 - c. Billing
 - d. Claims Management
 - e. Collections
 - f. Medical Necessity Reviews and Utilization Reviews

3. Examples of Healthcare Operations
 - a. Conducting quality assessment and improvement activities.
 - b. Reviewing the competence and qualifications of healthcare professionals or evaluating practitioner or provider performance.
 - c. Engaging in accreditation, certification, licensing, or credentialing activities.

- d. Conducting or arranging for medical review, legal services, and auditing functions.
- e. Engaging in business management and general administrative activities.

¹Use means sharing, employing, applying, utilizing, examining, or analyzing PHI within IDG

²Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG.

³Protected Health Information (“PHI”) contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

⁴Treatment means the provision, coordination, or management of healthcare and related services by IDG.

⁵Payment means activities undertaken by IDG to obtain payment or reimbursement for the provision of healthcare by IDG

⁶Healthcare Operations means services or activities that are necessary (and to the extent necessary) for IDG to carry out its functions as a healthcare provider.

⁷Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

Related Policies:

Permitted Uses/Disclosures of PHI-CC-P-004

Minimum Necessary Requirements-CC-P-006

De-Identifying PHI-CC-P-015

**Corporate Compliance Policies and Procedures
Integrated Dermatology, LLC**

Policy Number:	CC-P-022
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Patient's Right to Access Protected Health Information ("PHI") ¹
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce², independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

IDG shall afford individuals the right to access, inspect, and obtain a copy of their PHI in accordance with the provisions of the HIPAA Privacy Rule.

Policy & Procedure:

1. An individual who seeks to access his or her PHI must complete the Authorization for Release of Information form and submit it to IDG. The individual can obtain the form from the local office or IDG Privacy Officer.
 - a. Employees are required to follow the same procedures as any other patient and may NOT access their own records without an authorization.
 - b. The completed form should be forwarded to the local office, who will determine, with the Privacy Officer, whether to grant or deny the individual's request in accordance with the rules set forth in this policy.
2. IDG will respond to the request within 15 days. IDG may extend the deadline once for not more than 30 days by providing the patient with a written statement of the reasons for the delay and the date in which IDG will complete the request.
3. Granting Access
 - a. If IDG determines access may be granted we will provide the individual with access to or a copy of the record.
 - b. The individual is permitted to take notes on the record being viewed as well as capture images from their own record.

4. Denying Access
- a. If a request for access to PHI is denied, the patient, patient's personal representative or legal representative is entitled to a written notice of denial. The patient or his or her personal or legal representative may request a review of some denials, others are not reviewable.
 - b. Unreviewable-An individual does not have the right to access or request a review of the following information:
 1. Psychotherapy notes
 2. Information compiled in anticipation of civil, criminal, or an administrative action or proceeding.
 3. Health information that is subject to the Clinical Laboratory Improvement Amendment ("CLIA") to the extent allowing the access to the individual would be prohibited by law.
 4. Health information that was obtained from another person (other than a healthcare provider) under a promise of confidentiality and granting access would likely reveal the source's identity.
 - c. Reviewable-Access may be denied for the following reasons but must give the individual a chance to seek a review of the denial:
 1. A physician chosen by the facility has determined that access is likely to endanger the life or safety of the patient or another individual.
 2. When the health information sought makes reference to another person and a physician chosen by the facility determines that access is likely to cause harm to that person.
 3. When the request for access is made by a personal or legal representative and a physician chosen by the facility by IDG determines that providing access to the representative is likely to cause harm to the patient or another person.
 - d. Denial Notice-If IDG denies access for any reason, IDG must provide the patient with a written denial using the form entitled "Response to Patient's Request to Access and/or Copy Health Information", which includes:
 1. The basis for the denial
 2. A statement of the individual's right to have the denial reviewed and how such right may be exercised
 3. A description of how the individual can file a complaint with IDG and the Secretary of Health and Human Services. The description must include the name (or title) and telephone number of the person or office responsible for receiving complaints.

¹Protected Health Information (“PHI”) contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

²Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

Related Forms:

Authorization for Release of Information Form

Response to Deny Patient’s Request to Access and/or Copy Health Information

Related Policies:

Authorization for Use and Disclosure of Protected Health Information-CC-P-002

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-023
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Complaint and Reporting
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce¹, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

Patients (or representatives) and workforce members are encouraged to make complaints regarding suspected privacy violations. The intent of this policy is to promptly resolve complaints and mitigate the harmful effects or any privacy violation.

Policy & Procedure:

1. Patient Privacy Complaints
 - a. The Privacy Officer (or delegate) will supervise the investigation and resolution of all patient complaints, regardless of how the complaint was communicated.
 - b. Patient privacy complaints involve the following types of issues:
 1. Any alleged inappropriate use² or disclosure³ of Protected Health Information ("PHI")⁴.
 - a. Example: a complaint that IDG released billing records to a third party without a patient's written authorization
 - b. Example: a complaint that a IDG workforce member viewed a patient's medical record without a IDG business purpose
 2. A complaint that IDG has denied a patient's right to inspect PHI.
 3. A complaint that IDG has denied a patient's right to request an account of certain disclosures of PHI.
 4. A complaint that IDG has denied a patient's right to request amendments to PHI.
 5. A complaint that IDG has denied a patient's right to request restrictions on how IDG uses or discloses PHI.
 6. A complaint that IDG has denied a patient's right to request a change in how IDG communicates with him/her.

7. A complaint that IDG has denied a patient's right to request a copy of the IDG's Notice of Privacy Practice ("NPP")⁵
 8. If a patient privacy complaint is received by someone other than the Privacy Officer, the complaint must be forwarded promptly to the IDG Privacy Officer for review and investigation.
2. **Members of the Workforce Privacy Complaints**
- a. The IDG Privacy Officer (or delegate) will supervise the investigation and resolution of all workforce members' complaints, regardless of how the complaint was communicated.
 - b. Members of the workforce may file a complaint by:
 1. Contacting the Privacy Officer directly
 2. Contact the Compliance Hotline (833-920-0006)
 3. Contacting the Compliance Officer
 4. Contacting their immediate supervisor or other manager
 5. Contacting Human Resources
 - c. Workforce member's anonymity will be protected to the extent allowed by law. All complaints will be treated as confidential.
 - d. The Privacy Officer, together with the Compliance Officer through new hire orientation and annual education requirements will educate individuals and workforce members of their reporting obligation and how to file a complaint.
-

¹Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

²Use means sharing, employing, applying, utilizing, examining or analyzing PHI within IDG

³Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG.

⁴Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

⁵Notice of Privacy Practice (NPP) is a general description of the patient's rights with respect to PHI, how IDG may use and disclose PHI and IDG's legal duties with respect to PHI.

Related Forms:

Notice of Privacy Practice (NPP)

Related Policies:

Privacy Officer-CC-P-003

Permitted Uses/Disclosures of PHI-CC-P-004

Notice of Privacy Practice-CC-P-007

Patient Right to an Accounting of Disclosures of PHI-CC-P-010

Patient Right to Request an Amendment of PHI-CC-P-012

Resources

45 CFR §164.530-Administrative Requirements

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-024
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Breach Notification
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce¹, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

A breach is any unauthorized acquisition, access, use² or disclosure³ of Protected Health Information ("PHI")⁴. That compromises the security of privacy of such information and poses a significant risk of financial, reputational or other harm to the individual.

IDG notifies patient who are affected by a breach of Unsecured Protected Health Information⁵ without unreasonable delay and in no case later than 60 days after the breach is discovered.

A breach is considered discovered on the first day on which any individual, including the person who caused the breach, knew that a breach of Unsecured PHI has occurred.

Workforce members and those who provide services to or on behalf of IDG will immediately report any breach of Unsecured PHI or a situation that involves the loss or theft of an electronic device containing PHI or a suspected Information Security Incident⁶ to the IDG Privacy Officer by emailing the Privacy Officer at IDGCompliance@mydermgroup.com or IT Security by emailing IT@mydermgroup.com or calling the Compliance Hotline at 833-920-0006.

The IDG Privacy Officer (or delegate) is responsible for prompt investigation of all reported and discovered breaches of Unsecured PHI, which includes managing the breach investigation, coordinating with other IDG departments as necessary, completing a risk assessment and accurately reporting any breach of unsecured PHI to patients the US Department of Health and Human Services (HHS).

The IDG Security Officer (or delegate) is responsible for responding to all reported and discovered Information Security Incidents and performing any necessary analysis to determine whether an Information Security Incident has caused a breach of Unsecured PHI. When reporting breaches, IDG will follow all applicable federal and state laws.

All documentation relating to a breach investigation, including the risk assessment and any written notice of a breach, shall be maintained for a minimum of six (6) years.

Policy & Procedure:

1. **Duty to Report Suspected Breaches or Information Security Incidents**
 - a. Workforce members and those who provide services to or on behalf of IDG will immediately report any breach of Unsecured PHI to the IDG Privacy Officer. Loss or theft of an electronic device containing PHI or the security of PHI also should be reported by:
 1. Calling the IDG Hotline at 833-920-0006
 2. E-mailing the Privacy Officer at IDDGCompliance@mydermgrou.com
2. **Investigating Reported or Suspected Breaches of Unsecured PHI or Information Security Incidents**
 - a. The IDG Privacy Officer (or delegate) is responsible for prompt investigation of all reported and discovered breaches of Unsecured PHI, which includes managing the breach investigation, coordinating with other IDG departments as necessary, completing a risk assessment and accurately report any breach of unsecured PHI to patient an HHS.
 1. If a workforce member is involved in, or possibly responsible for the breach, the IDG Privacy Officer will contact the Human Resource Department to assist with the investigation and corrective action as needed.
 - b. The IDG Security Officer (or delegate) is responsible for responding to all reported and discovered Information Security Incidents and performing any necessary analysis to determine whether an Information Security Incident has caused a breach of Unsecured PHI. If there is a reasonable basis to believe that an Information Security Incident may have caused a breach of Unsecured PHI, the IDG Security Officer will notify the Privacy Officer.
 - c. The IDG Executive Leadership (or delegate) is responsible to communicate any required breach notification to the media.
 - d. Legal Counsel is responsible for any communications with law enforcement regarding a breach of Unsecured PHI.

3. Notification to Patients of Breaches of Unsecured PHI
 - a. After a complete investigation, and the outcome is a breach, IDG will notify patients who are affected by a breach of Unsecured PHI without unreasonable delay and in no case later than 60 days after the breach is discovered.
 1. If the patient is deceased, notice will be provided the patient's next of kin or personal representative.
 2. If the patient is incapacitated or incompetent, notice will be provided to the patient's personal representative.
 3. If the patient is a minor, notice will be provided to the patient's parent or guardian.
 - b. Written breach notices are provided in plain language at an appropriate reading level with clear syntax and language with no extraneous materials, in accordance with the Americans with Disabilities Act (ADA) and Limited English Proficiencies (LEP) requirements.
 - c. Written breach notices are sent by first-class mail to the last known address of the patient or other authorized individual reference in Section 3a.
 - d. When IDG has insufficient or outdated contact information:
 1. In situations involving less than 10 individuals, IDG uses a substitute form of notice, such as a telephone call.
 2. In situations involving 10 or more individuals, IDG must:
 - a. Post a conspicuous notice for 90 days on the IDG homepage that includes a toll-free number or
 - b. Provide notice in a major print or broadcast media in the geographical area where a patient can learn whether or not their Unsecured PHI is possibly included in the breach. A toll-free number must be provided in the notice.
 - e. If IDG determines that a patient should be notified immediately of a breach because of possible imminent misuse of Unsecured PHI, IDG will contact the patient by telephone or other means, as appropriate.
 - f. IDG will comply with any appropriate written request by law enforcement to delay the notification. IDG is required to document the statement and the identity of the law enforcement official and delay the notification for no longer than 30 days, unless a written statement from the law enforcement official states otherwise.
 - g. Regardless of the method by which notice of a breach of Unsecured PHI is provided, the breach notice will include:
 1. A brief description of what happened, including the date of the breach and the date of the discovery, if know.
 2. A description of the type of Unsecured PHI that was involved in the breach, such as full name, SS#, date of birth, home address, account number, diagnosis/treatment information, etc. Only the PHI description will be listed, not the patient's actual PHI.

3. The steps the individual should take to protect themselves from potential harm from the breach.
 4. A brief description of what IDG is doing to investigate the breach, mitigate the harm the individual and to protect against any further breaches.
 5. Contact procedures for individuals to ask questions or learn additional information, such as a telephone number, email address, website or postal address.
4. Notification to HHS of Breaches of Unsecured PHI
 - a. When a single breach involves 500 or more individuals, IDG provides notice to HHS without reasonable delay and in no case later than 60 days after a breach is discovered.
 - b. For breaches involving less than 500 individuals, IDG will submit an electronic log of calendar year breaches to HHS no later than 60 days after the end of the prior calendar year.
 - c. The IDG Privacy Officer is responsible for maintaining an accurate log of all breaches of Unsecured PHI that occurred at IDG during the calendar year.
 5. Notification to the Media of Breaches of Unsecured PHI
 - a. When a single breach of Unsecured PHI involves more than 500 individuals of the same state or jurisdiction, IDG shall provide notice to a prominent media outlet.
 - b. Executive Leadership is the only sources authorized to provide a notice to the media regarding a breach of Unsecured PHI on IDG's behalf.

¹Workforce member means IDG employees, volunteers, trainees, contractors and/or subcontractors whose conduct, in performance of work for IDG, is under direct control of IDG.

²Use means sharing, employing, applying, utilizing, examining or analyzing PHI within IDG

³Disclosure means the release, transfer, provision of, access to, or divulgence of PHI to a person or entity outside of IDG.

⁴Protected Health Information ("PHI") contains identifiers that can identify a patient or for which there is a reasonable basis to believe that information can be used to identify a patient, such as demographic or insurance information, medical record number, physician, admission date or photographic image. It can be in electronic, written, or oral form.

⁵Unsecured PHI is PHI that is not encrypted or rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS

⁶An Information Security Incident is a situation in which a IDG employee is aware of circumstances which may permit unauthorized access, use, disclosure, modification or destruction of electronic PHI.

Related Forms:

HIPAA Breach Investigation Form

Related Policies:

Privacy Officer-CC-P-003

Resources

45 CFR §160 and §164

Corporate Compliance Policies and Procedures Integrated Dermatology, LLC

Policy Number:	CC-P-025
Policy Section:	Corporate Compliance-HIPAA Privacy
Subject:	Social Media Use Policy
Effective:	11/1/21
Approval:	10/22/21
Reviewed:	8/23/22
Revised:	8/23/22

Scope:

This policy applies to all Integrated Dermatology, LLC ("IDG"), and its affiliates, subsidiaries, and their respective directors, officers, members of the workforce¹, independent contractors, and agents, including, where appropriate, others who provide services to or on behalf of IDG.

It is the policy of IDG that all reasonable use of Social Media Platforms is permitted under the terms set forth herein. This Policy is intended to protect IDG, its affiliated entities, and the practices with respect to their confidential information, including but not limited to, Protected Health Information ("PHI")², and trade secret information.

Policy & Procedure:

1. Workforce members
 - a. General Restrictions
 1. IDG urges all Workforce members **not** to post information regarding IDG, its affiliates, the practices, other Workforce members, or information about their role within IDG, which could lead to morale issues in the workplace or detrimentally affect IDG's business. This can be accomplished by always thinking before you post, being civil to others and their opinions, and not posting personal information about others unless you have received their permission. Workforce members are personally responsible for the content they publish on Social Media Platforms. Workforce members should be mindful that what they publish will be public for a long time. Workforce members should also be mindful that if IDG receives a problem, concern, or complaint from another Colleague about information that has been posted about that Colleague, IDG may need to investigate that problem, concern, or complaint, as appropriate under the circumstances, in order to ensure that there has been no violation of this Policy, IDG's Anti-Discrimination, Harassment and Retaliation Policy or other company policy. In the event that such a problem, concern or complaint is raised, you will be expected

to cooperate in any investigation of that problem, concern, or complaint,

2. Workforce members may not publish any content related to patients or patient care and must maintain strict adherence to all laws and policies related to a patient's personal health information. This includes, but is not limited to, patient name, photos, diagnostic testing results/images, case information, or any information that may lead a reasonable person to be able to identify a patient, etc. Even seemingly vague descriptions of patient interactions may present potential HIPAA violations where there are reasonable bases to believe that the information disclosed could allow someone to identify the patient. As a result, information or comments about patients or patient care are never appropriate or permitted.
3. Workforce members must not post business confidential information, as defined in Section B(2)(b) of this Policy, of IDG, or any of its affiliates, subsidiaries, or companies with which IDG does business, on any Social Media Platform. This prohibition applies, in particular, to postings on message boards and other sites oriented to investing or IDG's shareholders. Unauthorized disclosure of business confidential information also constitutes a violation of IDG's Code of Conduct. It should be noted that the prohibition against disclosing business confidential information on Social Media Platforms applies even to "anonymous" postings.
4. Workforce members should not use work time to update or monitor Social Media Platforms unless that activity is specifically part of the Workforce member's work duties.
5. Workforce members must not provide medical, or health advice purported to be from or on behalf of IDG on any Social Media Platform. In this regard, Workforce members must never offer comments, or respond to comments or questions, involving medical or health care advice over Social Media.
6. If you communicate about IDG's products or services on a Social Media Platform, you must disclose your connection as an employee of IDG and must state that your views express your personal opinions and do not reflect those of IDG. Workforce members should exercise good judgment on any postings and strive to be accurate, fair, and responsible in their communications. Persons who identify themselves on a Social Media Platform as employed by IDG must not under any circumstances purport to comment on behalf of IDG on major business or financial developments at IDG. Workforce members are reminded that only authorized spokespersons are authorized to speak on behalf of IDG to the public.

- b. Exceptions to the General Restrictions
 - 1. If Workforce members wish to use Social Media Platforms and technologies to promote a provider and/or a practice, they must consult the practice manager for that practice or someone from IDG's Human Resources Department for approval and to determine the appropriate strategy and tools for your audience and mission.
 - 2. Workforce members shall notify their practice manager, IDG's IT Department and IDG's HR Department to have either (i) the Workforce member's personal account added to the social media directory or similar tracking tool (if the Colleague wishes to post content to their personal social media page), or (ii) the Workforce member's name added to the list of individuals with access to a given practice's social media account (if the Workforce member will be managing a practice's social media page).
 - 3. Workforce members must ensure they have received permission to use any trademarked images and logos.
 - 4. Similarly, if there is any Protected Health Information, including a patient's likeness, name, procedure, or other identifiable information, Workforce members must ensure they have obtained the patient's permission in writing to use their likeness, and retain a copy of such permission on file.
- 2. Enforcement
 - a. Workforce members who participate in electronic communication in violation of this Policy or other applicable IDG rules of conduct may be subject to disciplinary action, up to and including termination of employment.
 - b. Specifically prohibited communications include but are not limited to:
 - 1. Any information of comments related to patients or patient care.
 - 2. Business confidential information including marketing plans, business strategic initiatives, client/customer lists, pricing information, product and services information, research and development activities, company financial information, trade secrets or other proprietary information relating to products, services, processes, know-how, designs, formulas, computer programs, technologies, systems and databases, or other internal information, as well as personal Colleague information (such as medical information, date of birth, social security number, and other personally identifiable information)
 - 3. Communication which defames or libels others

4. Communication that disparages others based upon a person's race, creed, color, sex, pregnancy, gender identity or expression, age, religion, national origin, nationality, marital status, domestic partnership status, civil union status, affectional or sexual orientation, ancestry, atypical hereditary cellular or blood trait, genetic information, political belief or activity, liability for service in the Armed Forces of the United States, military status or service, disability, AIDS/HIV status, sickle cell or hemoglobin C trait, relationship or association with a disabled person, use of a service animal, GED rather than high school graduate status, lawful use of a product when not at work or any other basis prohibited by applicable federal, state or local law.
5. Communication that constitutes threats of physical harm to Workforce members employed by IDG, threats to engage in violence of any kind or threats to engage in any other illegal conduct.
6. Communication that violates IDG's Anti-Discrimination, Harassment and Retaliation Policy or otherwise harasses or intimidates Workforce members of IDG to connect or communicate via Social Media.

Related Forms:
Code of Conduct